

DATA PRIVACY & CYBERSECURITY

HBS works alongside businesses of all sizes and across industries to safeguard data, protect privacy, identify potential weaknesses, and reduce the likelihood of breaches.

[OVERVIEW](#) | [NEWSLETTER](#) | [FOCUS](#) | [BLOG](#) | [IN THE PRESS](#)

Overview

As businesses continue to increase their use and storage of personal information and other data, it is more important than ever that they assess how they manage and control their data. HBS can assist with the preparation and implementation of proactive compliance plans not only to comply with relevant privacy laws and regulations but also to work towards a Strategic Privacy by Design plan for your business.

HBS can provide you with proactive strategies to reduce the likelihood of a security breach along with remedies to reduce your loss exposure should your data be compromised. We have a team of data privacy and cybersecurity attorneys throughout our offices to work with clients throughout the country.

Privacy

Electronic transfer of data and “cloud computing” reach across geographical boundaries in the global marketplace. While most jurisdictions have some level of data privacy laws, these laws can vary widely from one state or country to another. This creates a maze of compliance and privacy risk issues.

HBS can identify the data privacy laws applicable to your business and develop a proactive plan to comply with these laws.

Leadership



Richard Sheinis

Partner | Charlotte Office

T: [980.859.0380](tel:980.859.0380)

E:

rsheinis@hallboothsmith.com

[Full Team](#)

Podcast

HALL BOOTH SMITH, P.C.

Specifically, HBS can assist with:

- National compliance programs and policies to address CCPA, Colorado Privacy Act, Virginia Consumer Data Privacy Act, HIPAA, NY SHIELD Act, PCI-DSS, COPPA, and GLBA
- International compliance programs and policies to address GDPR, PIPEDA, and the national data privacy laws of many other countries
- Website and mobile application privacy compliance
- vDPO services
- Data subject access and opposition rights
- Audits and data mapping
- Drafting and negotiation of all manner of technology contracts



Blog

DATA PRIVACY & CYBERSECURITY



[Subscribe to Our Blog](#)

Related Services

[Business Transactions](#)

[Corporate & Partnership](#)

[Intellectual Property](#)

[International Business](#)

[Real Estate](#)

Strategic Privacy by Design

It is no longer enough to reactively implement compliance measures when laws and regulations are passed. By implementing a Strategic Privacy by Design program in your business, we address privacy proactively by incorporating privacy requirements with your business strategy. At HBS we believe businesses can achieve their goals while maintaining the privacy of personal information.

Security

If a data security breach has occurred the cost can be high, not just in terms of dollars but in terms of your integrity and brand. Proactive measures HBS can assist with include:

- Determining the personal information your business handles.
- Completing a proactive tabletop security assessment to find and address any gaps in your data security scheme.
- Assisting with data minimization strategies to reduce risk exposure.
- Prioritizing your privacy resources based on your risks.
- Instituting a security quality assessment and improvement

HALL BOOTH SMITH, P.C.

- plan.
 - Developing a data breach incident response plan.
-

Newsletter

Our Global Data Download: Data Privacy & Security Report newsletter provides monthly updates on trending cybersecurity and related news topics. Subscribe to the email list using the button below to stay updated with our most recent blogs, useful articles our team members have sourced, and other relevant material.

[Subscribe to Our Newsletter](#)

Archive

Past versions of Global Data Download are linked below, with the most recent editions listed first.

2024

- [Global Data Download: April 2024](#)
 - [Global Data Download: March 2024](#)
 - [Global Data Download: February 2024](#)
 - [Global Data Download: January 2024](#)
 - [Global Data Download: December 2023](#)
-

Podcast

HALL BOOTH SMITH, P.C.



Our *PrivacyCafé* podcast explores the complex and ever-changing landscape of data privacy, cybersecurity, and technology.

PrivacyCafé unravels the complexity of data privacy laws, offers insights on cybersecurity, discusses fast-moving artificial intelligence technologies and their implications, and interviews top experts. The conversation is brought to you by the firm's Data Privacy and Cybersecurity group. *PrivacyCafé* is essential listening for business owners, executives, board members, and anyone interested in the latest insights on these topics. *PrivacyCafé* is carried by the [Business RadioX®](#) network and can be found on all the major podcast apps.

Interested in speaking on our podcast? Connect with us at PrivacyCafé@hallboothsmith.com.

PrivacyCafé: **Analysis &** **Implications** **of the EU AI**

Act

April 1, 2024

Richard Sheinis and Jade Davis discuss the European Union's Artificial Intelligence Act and its implications for businesses globally, especially in the USA.

[Read Full Article](#)

PrivacyCafé: Predictions for 2024 in Data Privacy & Cybersecurity

March 6, 2024

Partners Richard Sheinis and Jade Davis discuss their predictions for the data privacy and cybersecurity industry in 2024.

[Read Full Article](#)

HBS Partners Richard Sheinis & Jade Davis Host New Podcast

“PrivacyCafé”

February 26, 2024

Hall Booth Smith is proud to announce the launch of its new podcast PrivacyCafé, hosted by Partners Richard Sheinis and Jade Davis.

[Read Full Article](#)

[Load More Posts](#)

Blog



The [Data Privacy & Cybersecurity Blog](#) explores legal developments, trends, and business strategies around data protection, retention, privacy, reporting obligations, risk management, how to respond to hacking or security breaches, what to disclose and when, and other agenda-setting topics.

The blog features tips to help clients identify data protection concerns, assure that their businesses are in compliance, and develop proactive plans that reduce the risk of data security breaches. We also weigh in on breaking news such as cyberattacks, ransomware, phishing, viruses, and other matters.

A Quick & Easy Guide to California's Suite of Proposed AI Regulations

April 3, 2024

California rolled out 31 new Artificial Intelligence bills affecting almost every level of commerce. Find out how they may affect your business, human resource operations, healthcare, schools, and more.

[Read Full Article](#)

Navigating the Updated OCR Guidance on Online Tracking Technologies: Key Insights

April 2, 2024

The recent update issued by OCR on March 18, 2024, revised the initial guidance from December 1, 2022, providing clearer directives

HALL BOOTH SMITH, P.C.

for HIPAA covered entities
and business associates
regarding the deployment of
online tracking tools.

[Read Full Article](#)

A Closer Look: EU's Finalized AI Act & What It Means for the U.S.

March 20, 2024

Touted as the world's first
comprehensive legal
framework of its kind, the AI
Act will go into effect in
stages over the next three
years. The AI Act will apply to
both businesses operating
within the EU and to any AI
developers or creators whose
AI systems are used in EU
countries and raises a few
questions...

[Read Full Article](#)

Meta's "Pay or Consent" Model Instills Consumer

Protection **Issues in** **European** **Union**

March 7, 2024

The EU Consumer Protection Agency has rallied against Meta's "Pay or Consent" model, claiming it is entirely too aggressive and coercive, fundamentally undermining the principles of GDPR.

[Read Full Article](#)

Compromise **Brings EU** **Artificial** **Intelligence** **Act One Step** **Closer to Final**

March 6, 2024

On February 13, 2024, EU member states voted unanimously in favor of the proposed EU AI Act, the result of extensive negotiations and compromises between member states and is now expected to be formally adopted in March or April of this year.

[Read Full Article](#)

LockBit **Takedown &** **Pseudo-** **Reemergence** **Continue to** **Crystallize the** **Economic** **Impacts of** **Ransomware-** **as-a-Service**

March 6, 2024

In the ongoing global hunt for cybercriminals, the past thirty days have been illuminating for some, unsurprising for others, and climactic for all following the takedown of LockBit.

[Read Full Article](#)

FTC Moves to **Modernize** **Children's** **Online Privacy** **Protection**

Rule

February 7, 2024

After almost four years of review and 175,000 public comments later, the FTC unveiled its plan to update the Children's Online Privacy Protection Rule (COPPA Rule) on December 20, 2023, after the Commission voted 3-0. The last COPPA revision was made in 2013...

[Read Full Article](#)

EU's Cookie Reduction Pledge: How It Affects Your Business

February 7, 2024

The EU's cookie reduction pledge represents a significant move towards enhanced digital privacy. While offering more control over cookies, the emergence of alternative tracking methods like device fingerprinting and contextual targeting highlights new complexity, reminding companies that users are no longer data-naïve.

[Read Full Article](#)

Forecasting 2024 Global Privacy Legislative Developments

February 6, 2024

Global legislative developments in the privacy sphere were abundant in 2023. Privacy professionals from around the world predict that legislation pertaining to data privacy and cyber security will continue to flourish in 2024, and this post explores those predictions.

[Read Full Article](#)

The World's First Comprehensive AI Law — the EU AI Act — is a Landmark in AI Regulation

January 19, 2024

Globally, business owners are asking how the European

HALL BOOTH SMITH, P.C.

Union's AI Act affects their business. This article will delve into the Act and how businesses will be affected globally, with an emphasis on the U.S.

[Read Full Article](#)

HHS Warnings Trigger Class Actions Against Medical Providers for Use of Online Tracking Technologies

January 2, 2024

After roughly a year of multiple warnings by the HHS concerning the usage of online tracking technologies and associated privacy and security risks, class action lawsuits have begun to be filed...

[Read Full Article](#)

The FTC Shows Its

Dislike of **Facial** **Recognition** **Technology**

January 2, 2024

In May 2023, the FTC issued a warning that it would be closely monitoring the use of biometric information technology, including those powered by machine learning, because they raise significant consumer privacy and data security concerns and have the potential for bias and discrimination. On December 19, the FTC made good on its promise by

[Read Full Article](#)

California **Privacy** **Protection** **Agency Board** **Approves** **Legislative** **Proposal to** **Require** **Browsers to**

Offer Opt-out Preference Signals

December 20, 2023

On December 8, 2023, the California Privacy Protection Agency (CPPA) Board voted 5-0 at its meeting to advance a legislative proposal to require browser vendors to include a feature that allows users to exercise their California privacy rights through opt-out preference signals. This recent unanimous decision marks a significant stride toward fortifying consumer privacy rights in the digital realm

[Read Full Article](#)

Justice Department Disrupts Prolific AlphV/Blackcat Ransomware Variant

December 19, 2023

On December 19, 2023, the FBI announced its investigation into Blackcat

group, also known as AlphV or Noberus, and that it gained visibility into AlphV's computer network due in part to assistance provided by an informant. "Law enforcement engaged a confidential human source who routinely provides reliable information related to ongoing cybercrime investigations," the FBI

[Read Full Article](#)

Another Year Wasted for U.S. Federal Data Privacy Legislation

December 5, 2023

As the rest of the world continues to move forward with national data privacy legislation, the United States continues its well-established habit of proposing piecemeal data privacy laws that go nowhere

[Read Full Article](#)

California Privacy

Protection **Agency (CPPA)** **Publishes** **Revised Draft** **Cybersecurity** **Audit** **Regulations in** **Advance of** **December** **Board Meeting**

December 5, 2023

On November 8, 2023, the CPPA published an updated draft of its cybersecurity audit regulations, intended, in part, to facilitate board discussion and public participation during the upcoming CPPA board meeting...

[**Read Full Article**](#)

EU-UK Data **Privacy Round** **Up**

December 5, 2023

November was a busy month for data privacy. See below for updates to the EU AI Act, the Information Commissioner's Office's (ICO)

response regarding third party cookies, the ICO's appeal of Clearview ruling, and the Italy data protection authority's (DPA) training probe

[Read Full Article](#)

HHS Publishes New Cybersecurity Resources

May 5, 2023

The U.S. Department of Health and Human Services (HHS) Office of Information Security recently published new cybersecurity resources with the goal of mitigating common cybersecurity threats in the health care sector. HHS Resources Webinars: These are spotlighted periodically and noticed to subscribers. The next webinar spotlights Health Industry Cybersecurity Practices 2023 changes as it relates

[Read Full Article](#)

Not Sneaky Enough:

Google Pays \$391.5M Privacy Violation Settlement

December 7, 2022

Written by: Savannah Liner
Avera, Esq. Connecticut
Attorney General William
Tong announced a historic
settlement with Google
regarding its predatory
disregard for users' location
tracking preferences. Google
will pay \$391.5 million to 40
states in a privacy violation
settlement for continuing to
track users after opting out of
a feature called location
history. Background This

[Read Full Article](#)

Canada's Consumer Protection Privacy Act (CPPA) at Least One Year Away

November 8, 2022

HALL BOOTH SMITH, P.C.

Written by: Richard Sheinis,
Esq. Canada's Federal Privacy
Law, the Personal Information
Protection and Electronics
Documents Act (PIPEDA) is
over 22 years old. Its
replacement, proposed Bill
C-27, which introduces the
Consumer Protection Privacy
Act (CPPA) is still at least one
year away from being passed.
The CPPA is part of Canada's
Digital Charter
Implementation

[Read Full Article](#)

European Union Considering a Complete Ban on Facial Recognition Technology

October 11, 2022

Written by: Gabriel Lopez,
Esq. Earlier this month,
European Union (EU)
lawmakers began political
debate on the EU's Artificial
Intelligence Act (AI Act). The
legislation focuses on
regulating the use of artificial
intelligence in society. The AI
Act seeks to introduce legal
obligations commensurate

with the potential harm,
societal or otherwise, that
may come with

[Read Full Article](#)

Snapchat **Agrees to \$35** **Million** **Settlement** **with Illinois** **Residents**

September 20, 2022

Written by: Gabriel Lopez,
Esq. A \$35 million settlement
between the residents of
Illinois and Snapchat has
been reached following a
class action lawsuit over the
collection of biometric data.
According to the complaint
filed on May 11, 2022, for
alleged violations of Illinois'
Biometric Information Privacy
Act, the company allegedly
collected biometric data
through

[Read Full Article](#)

Virginia **Amends the** **Virginia**

Consumer Data Protection Act ("VCDPA")

April 19, 2022

Written by: Richard Sheinis, Esq. As many of you know, the VCDPA is scheduled to go into effect on January 1, 2023. In advance of the effective date, the Virginia Legislature has passed several amendments to the Act. The amendments are as follows: A new exemption to the right to delete when the personal data

[Read Full Article](#)

Shopify and Leger Facing Second Class Action Over 2020 Data Breach

April 19, 2022

Written by Joseph Stepina, Esq. Canadian e-commerce company, Shopify Inc., faces a new class action lawsuit over a 2020 data breach in

HALL BOOTH SMITH, P.C.

which hackers were able to access personally identifiable information of over 270,000 individuals. Shopify contracted with Leger, who sells SAS cryptocurrency hardware wallets, to store its customers' personal information. In addition, the hackers

[Read Full Article](#)

The FTC's Full-Court (Cafe)Press

April 19, 2022

Written by: Brock Wolf, Esq.
Last month, the Federal Trade Commission ("FTC") announced a proposed settlement with the online retailer of customized merchandise, CafePress. This settlement follows allegations that the company failed to implement reasonable security measures and attempted to cover up a 2019 data breach. The proposed settlement would call for CafePress to pay

[Read Full Article](#)

Indiana

Amends Its Data Breach Notification Law

April 19, 2022

Written by: Brock Wolf, Esq.
Indiana Governor Eric Holcomb signed into law an amendment to Indiana's data breach notification statute. The amendment, which takes effect on July 1, 2022, implements a forty-five (45) day deadline for reporting a breach to affected individuals and the Indiana Attorney General. Indiana's breach notification law now requires entities to

[**Read Full Article**](#)

Ransomware Group Conti Faces Data Leak of Its Own

March 16, 2022

Written by: Joseph Stepina, Esq. Notorious ransomware group Conti has, itself, been the target of cyberattacks after it announced its

HALL BOOTH SMITH, P.C.

allegiance to Russia and its support of Russia's ongoing invasion of Ukraine. Conti is famous for conducting ransomware attacks on a variety of business and governmental entities including Ireland's national health service, Shutterfly, and fashion

[Read Full Article](#)

U.S. Senate Unanimously Passes the Strengthening American Cybersecurity Act

March 16, 2022

Written by: Brock Wolf, Esq.
On March 1, 2022, the United States Senate unanimously passed the Strengthening American Cybersecurity Act.

This package of three bills aims to strengthen U.S. cybersecurity infrastructure by enhancing incident reporting requirements, tightening cybersecurity requirements for federal agencies and calling for federal agencies to migrate to cloud-based networks. One of

the

[Read Full Article](#)

California **Privacy Rights** **Act** **Regulations** **Delayed**

March 16, 2022

Written by: Brock Wolf, Esq.
Last month, on February 17, the California Privacy Protection Agency (“CPPA”) announced at a board meeting that the publication of final regulations under the California Privacy Rights Act (“CPRA”) will be delayed. Under the CPRA, regulations were to be finalized by July 1, 2022. The goal was to provide businesses

[Read Full Article](#)

Utah About To **Become The** **Fourth State** **To Pass** **Privacy Law**

March 16, 2022

Written by: Richard Sheinis,

HALL BOOTH SMITH, P.C.

Esq. On March 3, 2022 the Utah Consumer Privacy Act (“UCPA”) was passed by the Utah legislature and sent to the Governor to sign, which he is expected to do. Most of you will be familiar with the requirements of the UCPA as they are similar to recently passed privacy laws

[Read Full Article](#)

Fourth Time’s the Charm? Washington State Legislature Contemplating Comprehensiv e Data Privacy Bills

February 15, 2022

Written by: Brock Wolf, Esq.
Washington is among the states expected to pass a comprehensive data privacy law this year. At least, that has been the headline since 2019, when the Washington Privacy Act was first introduced in the legislature. Now, for the fourth year in a row, the legislature will attempt to pass a

[Read Full Article](#)

Illinois **McDonald's** **Enter \$50** **Million** **Settlement for** **Alleged BIPA** **Violation**

February 15, 2022

Written by: Brock Wolf, Esq.
Illinois' Biometric Information Privacy Act ("BIPA") is arguably the nation's strictest when it comes to biometric information. Biometric information protected by BIPA includes fingerprints, retina or iris scans, hand scans, facial recognition, DNA and other unique biological information. Passed in 2008, BIPA requires that before companies may collect or otherwise

[Read Full Article](#)

The **Algorithmic** **Accountability** **Act of 2022 Is**

Introduced

February 9, 2022

Written by: Richard Sheinis, Esq. Several Democratic legislators have introduced the Algorithmic Accountability Act of 2022 (the “Act”). This legislation is a redo of the 2019 Algorithmic Accountability Act. While this piece of legislation will likely die on the vine, like so many personal data related bills before it, it demonstrates a disturbing trend to

[Read Full Article](#)

The Turf War Over Personal Data Continues

February 2, 2022

Written by: Richard Sheinis, Esq. As many of our readers know, the transfer of personal data from the EU to countries outside the EU is heavily regulated by the GDPR. Companies that transfer personal data from the EU to the US typically use Standard Contractual Clauses, which are intended to provide some assurance that personal data

[Read Full Article](#)

Privacy Allegations Lead to \$18.4 Million in Settlements for Boston Hospitals

January 11, 2022

Written by: Brock Wolf, Esq.
Mass General Brigham
Incorporated and its affiliate
healthcare providers (“Mass
General”) agreed to pay
\$18.4 million to settle a class-
action against the healthcare
system. While healthcare
providers around the nation
are falling victim to data
breaches and ransomware
attacks, this lawsuit has a
different origin. Instead, this
class-action stems from

[Read Full Article](#)

European Cookie Rules Continue To Evolve

January 10, 2022

HALL BOOTH SMITH, P.C.

Written by: Richard Sheinis, Esq. CNIL, the French Data Privacy Supervisory Authority, has fined Google 150 Million Euros, and Facebook 60 Million Euros, for having websites that do not make refusing cookies as easy as accepting them. Prior GDPR guidance, and rulings from various supervisory authorities, required that websites using cookies have a cookie banner

[Read Full Article](#)

Indian Data Protection Bill Nearing Passage

January 7, 2022

Written by: Brock Wolf, Esq. Last month, India's Joint Parliamentary Committee submitted its report on India's draft Data Protection Bill (the "Bill") to Parliament. The report, which comes after two (2) years of deliberations, contains the Joint Parliamentary Committee's recommendations and a revised draft of the Bill. In 2017, the Supreme Court of India declared

[Read Full Article](#)

FTC Starts Process to Adopt Privacy Rules

December 21, 2021

Written by: Richard Sheinis, Esq. In September 2021, Senator Richard Blumenthal and eight other Democratic Senators sent a letter to FTC Chair Lina Kahn requesting that the agency begin a rulemaking process to address data privacy. Blumenthal and the other Senators stated that consumer privacy had become a consumer crisis with tech companies routinely breaking

[Read Full Article](#)

Log4j Vulnerability Sweeps the Globe

December 21, 2021

Written by: Brock Wolf, Esq. Earlier this month, on December 9, 2021, a critical vulnerability was discovered in the Apache Software

Foundation's ("Apache")
Log4j code, potentially
providing threat actors with
access to millions of
computers and devices
worldwide. On December 10,
the director of cybersecurity
at the National Security
Agency (NSA) and the
Department of

[Read Full Article](#)

New EDPB **Guidance on** **International** **Data Transfers**

December 21, 2021

Written by: Alyssa J. Feliciano,
Esq. The European Data
Protection Board ("EDPB")
released new guidelines in
November to clarify when a
processing operation should
be classified as an
international data transfer
based upon Article 3 and
Chapter V of the European
Union's ("EU") General Data
Protection Regulation
("GDPR"). The guidelines are
intended to create a

[Read Full Article](#)

California Continues to Update and Enforce Privacy Laws

November 9, 2021

Written by: Brock Wolf, Esq.
and Alyssa J. Feliciano, Esq.
California continues to update
its privacy policies. Changes
and clarifications are
constantly being announced,
making it imperative for
businesses to stay vigilant in
their practices. Notably, the
California Privacy Protection
Agency subcommittee (the
“Agency”), which was created
under the California Privacy
Rights Act (“CPRA”),
proposed

[**Read Full Article**](#)

Yet Another Senator Introduces Data Privacy Legislation

November 8, 2021

Written by: Richard Sheinis,
Esq. Last month I wrote about

the need for federal data privacy legislation. Although numerous Senators have introduced such legislation, nothing much seems to happen after the initial introduction. Adding to the list, Senator Catherine Cortez Masto (D-Nev.) is introducing the Digital Accountability and Transparency to Advance (DATA) Privacy Act. There

[Read Full Article](#)

Saudi Arabia **Passes** **Personal Data** **Protection** **Law**

November 2, 2021

Written by: Brett Lawrence, Esq. On September 16, 2021 by Royal Decree, Saudi Arabia implemented the Personal Data Protection Law ("PDPL"). The PDPL becomes effective on March 23, 2022 and will be enforced by the Saudi Data and Artificial Intelligence Authority ("SDAIA"). Regulated businesses have until March 23, 2023 before the PDPL is enforced. We

[Read Full Article](#)

Can't Congress Pass a Law for Data Privacy?

October 12, 2021

Written by: Richard Sheinis, Esq. The U.S. is lagging further and further behind the rest of the world when it comes to the privacy of personal data. The EU's General Data Protection Regulation (GDPR), which became effective in 2018, has become the "gold standard" for data privacy. Many countries have used the GDPR as the model

[**Read Full Article**](#)

Proposed Ransom Disclosure Act

October 11, 2021

Written by: Alyssa Feliciano, Esq. Representative Deborah Ross and Senator Elizabeth Warren proposed the Ransom Disclosure Act ("RSA"), to provide DHS with information regarding ransomware attacks and subsequent payments that are made by

covered entities. The goal of the RSA, according to Rep. Ross and Sen. Warren, is to provide DHS with data

[Read Full Article](#)

California **Privacy Update**

October 7, 2021

Written by: Brett Lawrence, Esq. 1. California's Genetic Information Privacy Act On October 6, 2021, California passed the Genetic Information Privacy Act ("GIPA"). Under GIPA, California residents have greater control over how their genetic information will be collected and used by specific companies. GIPA becomes effective on January 1, 2022. GIPA applies to "direct-to-consumer genetic testing

[Read Full Article](#)

EDPB **Releases** **Opinion on** **South Korea** **Draft**

Adequacy Decision

October 1, 2021

Written by: Alyssa Feliciano, Esq. On September 24, 2021, the European Data Protection Board (“EDPB”) released an opinion on the draft adequacy decision for South Korea, which in large part was positive for the country. There were certain areas of concerns that were pointed out by the EDPB. Once the EDPB’s stated issues are addressed

[Read Full Article](#)

China Passes the Personal Information Protection Law

September 14, 2021

Written by: Brett Lawrence, Esq. On August 20, 2021, China passed its Personal Information Protection Law (“PIPL”). This is China’s first general and broadly sweeping privacy law regulating the collection, processing, and transferring of personal

HALL BOOTH SMITH, P.C.

information, similar to the European Union's General Data Protection Regulation ("GDPR"). PIPL takes effect on November 1, 2021, less than

[Read Full Article](#)

[Irish DPA Fines Whatsapp \\$225 Million Euro For Transparency Violations](#)

September 14, 2021

Written by: Richard Sheinis, Esq. We are all aware of the requirements under several laws that a company's website must have a link to the company's privacy policy explaining how the company treats personal information. The oxymoronic part of the privacy policy requirement, however, is that laws require more and more information to be included

[Read Full Article](#)

[South Carolina](#)

Federal Court Denies Dismissal of CCPA Claims in Class Action

September 14, 2021

Written by: Alyssa Feliciano, Esq. A federal judge in South Carolina denied a motion to dismiss claims in a class action lawsuit brought under the California Consumer Privacy Act (“CCPA”). The class action suit was brought against Blackbaud, following a ransomware attack in early 2020 that left countless individual’s data compromised. Blackbaud attempted to have

[Read Full Article](#)

Federal District Court Rejects Plaintiff’s Attempt to Bring UK GDPR Lawsuit

in US Court

September 1, 2021

Written by: Alyssa Feliciano, Esq. On August 16, 2021, a California federal district court dismissed what would have been the first case brought by a British or EU resident to the US regarding the interpretation and enforcement of GDPR. The Plaintiff, a UK resident, alleged that US-based company, PubMatic, placed unique and therefore individuating identifiers

[Read Full Article](#)

California Requires Global Privacy Control Signals Opt- Out

August 10, 2021

Written by: Alyssa Feliciano, Esq. The CCPA gives authority to its Attorney General (“AG”) to determine how businesses must comply with the opt-out of the sale of personal information requirement under the law. California’s

recently inaugurated AG, Rob Bonta, announced that businesses will be required to accept Global Privacy Control (“GPC”) signals as an opt-out

[Read Full Article](#)

Uniform Law Commission Publishes Proposed Uniform Personal Data Protection Act

August 9, 2021

Written by: Brett Lawrence, Esq. In July 2020, the Uniform Law Commission (“ULC”) voted to approve and recommend the proposed Uniform Personal Data Protection Act (“UPDPA”). Like the Uniform Commercial Code, the UPDPA is a model law designed as a cut-and-paste piece of legislation that states can tailor and subsequently adopt to their liking. The ULC

[Read Full Article](#)

Amazon **Receives \$887** **Million EU** **Fine for Data** **Privacy** **Violations**

August 4, 2021

Written by: Alyssa Feliciano, Esq. On July 16, 2021, the EU's Commission Nationale pour le Protection des Données ("CNPD") fined Amazon the equivalent of \$887 million dollars after it determined that Amazon was processing personal data in violation of the GDPR.

Amazon representatives released a statement that the finding was without merit, citing that Amazon

[Read Full Article](#)

European Data **Protection** **Board Issues** **Guidance** **Clarifying** **Controller-**

Processor Relationship

August 2, 2021

Written by: Charles R. Langhorne IV, Esq. On July 7, 2021, the European Data Protection Board (“EDPB”) issued guidance further clarifying the relationship between controllers, joint controllers, and processors, under the General Data Protection Regulation (“GDPR”). This guidance is an update to the guidance issued by the Article 29 working party on February 16, 2010. The

[Read Full Article](#)

The European Protection Board Issues Guidance On Supplementary Measures For The Cross-Border Transfer Of Personal Data

July 13, 2021

HALL BOOTH SMITH, P.C.

Written by: Richard Sheinis, Esq. Most of you know that on June 4, 2021, the European Commission (“EC”) adopted two (2) new sets of Standard Contractual Clauses (“SCC”) for the cross-border transfer of personal data from the EU. The new SCC are due to a general need for updating the existing SCC, as well as

[Read Full Article](#)

New York City Passes Biometric Law

July 12, 2021

Written by: Brett Lawrence, Esq. and Alyssa J. Feliciano, Esq. On July 9, 2021, New York City’s biometric data law (the “Law”) became enforceable. The Law requires specific businesses to notify customers when their biometric data is being collected or shared. The Law further prohibits the selling of biometric data. Biometric Data Defined The Law defines

[Read Full Article](#)

Colorado

Privacy Act **("CPA")**

July 8, 2021

Written by: Charles R. Langhorne IV, Esq. and Alyssa J. Feliciano, Esq. CURRENT STATUS The Bill passed and has been signed by the Governor. EFFECTIVE DATE July 1, 2023 TO WHOM DOES CPA APPLY? The CPA applies if a business meets one the following circumstances:
Requirement 1: Conducts business in Colorado; or
Produces commercial products or services

[Read Full Article](#)

New York's **New Guidance** **on Preventing** **Ransomware**

July 2, 2021

Written by: Brett Lawrence, Esq. On June 30, 2021, the New York Department of Financial Services ("DFS") issued new guidance on ransomware prevention. Noting the increase in ransomware attacks and increases in the cost of cybercrime, DFS issued nine

(9) specific security controls that every business should implement to remove common weaknesses exploited by ransomware

[Read Full Article](#)

Nevada Amends Privacy Law for Opting Out of the Sale of Personal Information

June 8, 2021

Written by: Charles R. Langhorne IV, Esq. and Alyssa J. Feliciano, Esq. Nevada law already allows individuals to “opt out” of allowing a business to sell their personal information. On June 2, 2021, Nevada Governor, Steve Sisolak, signed SB 260, which amended the definition of “sale”. This change means that the existing law will become broader

[Read Full Article](#)

Representative

Ted Lieu Once Again Introduces The “Ensuring National Constitutional Rights For Your Private Telecommunic ations (ENCRYPT) Act”

June 8, 2021

Written by: Richard Sheinis,
Esq. This Bill was first
introduced in 2016 in
response to a dispute
between the FBI and Apple in
which the FBI sought to have
Apple provide access to the
locked mobile phone of a
suspect in a mass shooting in
San Bernardino, California.
The Act has been
reintroduced each year since

[Read Full Article](#)

EU Commission

Issues New Standard Contractual Clauses

June 5, 2021

Written by: Charles R. Langhorne IV, Esq. On June 4, 2021, the European Commission issued the long awaited new version standard contractual clauses (“SCCs”). In fact, the Commission issued two (2) different sets of SCCs. Governing transfers of personal data within the European Union. Officially cited as: C(2021) 3701. Governing transfers of personal data outside the

[Read Full Article](#)

President Biden Issues Executive Order Improving Cybersecurity

May 15, 2021

Written by: Brett Lawrence, Esq. On May 12, 2021, President Joe Biden signed an

HALL BOOTH SMITH, P.C.

executive order to improve the nation's cybersecurity and protect the federal government's networks (the "Order"). In their official statement, the White House expressly mentioned that the Colonial Pipeline and other cybersecurity incidents were "sobering reminders" that malicious cyber activity remains prevalent. The

[Read Full Article](#)

North Carolina **Introduces** **Consumer** **Privacy Act**

May 11, 2021

Written by: Charles R. Langhorne IV, Esq. On April 7, 2021, North Carolina joined the race to enact state privacy law, by introducing the North Carolina Consumer Privacy Act (the "Act"). The Act was introduced by Senators DeAndrea Salvador (D), Ben Clark (D), and Joyce Waddell (D). Notably, all of the sponsoring senators are Democrats, which

[Read Full Article](#)

Microsoft Allows Customers to Choose EU for Data Processing & Storage

May 10, 2021

Written by: Brett Lawrence,
Esq. On May 6, 2021,
Microsoft announced it will
allow its commercial and
public sector customers in the
European Union (“EU”) to
process and store all of their
personal data in the EU. This
implementation will be
completed by the end of 2022
and is called the “EU Data
Boundary for

[Read Full Article](#)

EDPB Adopts Two Opinions on the Draft UK Adequacy Decisions

May 5, 2021

Written by: Brett Lawrence,
Esq. On April 14, 2021, the

HALL BOOTH SMITH, P.C.

European Data Protection Board (“EDPB”) announced it had adopted two opinions in support of the draft UK adequacy decisions. The opinions stem from the EDPB’s review of the European Commission’s draft adequacy decisions for the General Data Protection Regulation (“GDPR”) and the Law Enforcement Directive (“LED”).

[Read Full Article](#)

The FTC Is Looking For Truth, Fairness, And Equity In The Use of Artificial Intelligence

May 3, 2021

Written by: Richard Sheinis, Esq. On April 19, 2021 the FTC issued what might be called guidance, but is more of a warning, regarding the use of artificial intelligence. The FTC cautions against using AI in a way that produces discriminatory outcomes. The FTC states

that in order to avoid bias
and prejudice, the data

[Read Full Article](#)

New York DFS Issues Cyber Insurance Risk Framework

April 13, 2021

Written by: Charles R.
Langhorne IV, Esq. Back in
March the New York
Department of Financial
Services (“NY DFS”) issued
Circular Letter No. 2 (2021)
providing guidance to
insurers offering cyber
insurance in New York. The
guidance provides a
framework that could very
well become required of
insurers at a later date. The
guidance urges

[Read Full Article](#)

Approved CCPA Regulations and

Appointees to CPRA Privacy Protection Agency

April 7, 2021

Written by: Brett Lawrence,
Esq. 1. CCPA Regulations
Effective as of March 15,
2021, California's Office of
Administrative Law approved
additional California
Consumer Privacy Act
("CCPA") regulations. The
regulations provide the
following: Offline Notification.
Any business who sells
personal information of a
consumer that has been
collected "offline" must
provide proper consumer
notification through an offline

[Read Full Article](#)

French Supervisory Authority To Enforce Its Ad Tracker ("Cookie") Guideline

April 2, 2021

HALL BOOTH SMITH, P.C.

Written by: Richard Sheinis,
Esq. As of April 1, 2021, the
French Supervisory Authority,
Commission Nationale de
l'Informatique et des libertes
("CNIL") will enforce its
cookie and ad tracker
guidelines. CNIL had
previously announced it
would give companies until
March 31, 2021 to adjust
their ad tracker and cookie
practices to come into
compliance. Most

[Read Full Article](#)

Federal **District Court** **Dismisses** **Walmart Data** **Breach Class** **Action**

April 1, 2021

Written by: Brett Lawrence,
Esq. On March 5, 2021, the
Federal District Court for the
Northern District of California
granted Walmart's motion to
dismiss the plaintiff's class
action lawsuit for exposed
customer personal data. This
was one of the first major
lawsuits alleging violations
under the California
Consumer Privacy Act

("CCPA"). We previously discussed this

[Read Full Article](#)

[Facebook Ordered to Pay \\$650 Million For Violation of Illinois' Biometric Information Privacy Act](#)

March 9, 2021

Written by: Richard Sheinis, Esq. The Biometric Information Privacy Act ("BIPA") is an Illinois statute that prohibits the use of biometric identifiers or information without prior notification and written consent. Facebook ran into trouble when a lawsuit was filed in 2015 alleging Facebook violated BIPA by tagging photos using facial recognition without their consent. Facebook

[Read Full Article](#)

[Brazil and EU](#)

Data Breach Notification Guidance

March 9, 2021

Written by: Brett Lawrence,
Esq. Brazil and the European
Union recently issued further
guidance on the procedures
for handling and reporting a
data breach. While Brazil
finally published guidance
before the law is to take
effect, the European Union
("EU") issued contextualized
guidance for the types of data
breaches that controllers
usually experience. Brazil
Brazil's data

[Read Full Article](#)

Canada Industry Group Releases Digital Advertising Policies

March 9, 2021

Written by: Charles R.
Langhorne, IV, Esq. In 2020,
Canada announced that its

legislature was planning to revamp the existing federal legislation (PIPEDA). The understanding is that it will lead to a more GDPR-esque framework of data privacy. The goal of these policies is to govern the direction of IAB Canada's role in shaping the

[Read Full Article](#)

Ecuador Data Privacy Law Debated in Congress

March 9, 2021

Written by: Brett Lawrence, Esq. Ecuador may soon be another country to enact general data privacy legislation. Introduced in September 2019, Ecuador's Data Protection Bill (the "Bill") nearly mirrors the European Union's General Data Protection Regulation ("GDPR"). The Bill has 76 articles and 12 chapters; we summarize some of the fundamental provisions below. Jurisdictional Reach

[Read Full Article](#)

5th Circuit Overturns \$4.3 Million HIPAA Penalty

February 9, 2021

Written by: Brett Lawrence, Esq. On January 14, 2021, the United States Court of Appeals for the 5th Circuit overturned a \$4.348 million fine issued by the Department of Health and Human Services (“HHS”) for alleged HIPAA violations against the University of Texas M.D. Anderson Cancer Center. Factual Background The case arose as a result

[Read Full Article](#)

FTC Settles Two Data Privacy Allegations

February 9, 2021

Written by: Brett Lawrence, Esq. Last month, the Federal Trade Commission (“FTC”) settled two allegations against two companies surrounding the unfair and deceptive use of facial

HALL BOOTH SMITH, P.C.

recognition software and disclosure of health data. Everalbum, Inc. The FTC alleged that Everalbum, Inc., a California-based developer of a photo app called “Ever,” deceived consumers about its use

[Read Full Article](#)

States Introducing Privacy Legislation

February 9, 2021

Written by: Charles R. Langhorne IV, Esq. 2021 is off to a hot start with many states introducing private sector privacy legislation. In this article I will outline:
Virginia Washington
Oklahoma New York
Minnesota Virginia Virginia
seems to be on track to win the race for the quickest to pass a privacy law. The Consumer

[Read Full Article](#)

What Is The Status Of

Personal Data Transfers Between the EU and the UK?

February 9, 2021

Written by: Richard Sheinis, Esq. On December 24, 2020, the EU-UK Trade Cooperation Agreement was announced. This Agreement contained an adequacy “bridge” so that the EU will treat the UK as an adequate jurisdiction for purposes of the protection of personal data for up to 6 months. During this period, the EU is to assess

[Read Full Article](#)

New York Proposes Biometric Privacy Law

January 12, 2021

Written by: Charles R. Langhorne IV, Esq. On January 6, 2021, New York legislators introduced the Biometric Privacy Act (“BPA”) to protect the rights of New York residents whose

biometric information has been collected, used, or stored by a private entity. Not surprisingly, BPA does not apply to state or local government entities. BPA imposes

[Read Full Article](#)

EU Council Releases Draft ePrivacy Regulation

January 12, 2021

Written by: Brett Lawrence, Esq. On January 5, 2021, the Council of the European Union released a new draft version of the ePrivacy Regulation. The draft regulation is intended to replace the current ePrivacy Directive since the European Commission approved the first draft ePrivacy Regulation back in January 2017. In fact, this new draft version

[Read Full Article](#)

No Solution Yet For The Transfer of

Personal Data from EU to the US

January 12, 2021

Written by: Richard Sheinis, Esq. The transatlantic transfer of personal data from the EU to the US is still a mess. Since the EU Court of Justice struck down the EU-US Privacy Shield in July 2020, and called into question the validity of the EU's standard contractual clauses, a solution to allow transfer of personal

[Read Full Article](#)

Proposed Changes to HIPAA Privacy Rule

January 12, 2021

Written by: Sean Cox, Esq. On December 10, 2020, the Trump administration announced proposed changes to the HIPAA privacy rule. According to the announcement, the changes are intended to “support individuals’ engagement in their care, remove barriers to

coordinated care, and reduce regulatory burdens on the health care industry.” The most important changes relate to

[Read Full Article](#)

Vodafone **Fined €12.25** **Million by** **Italian Data** **Protection** **Authority**

December 8, 2020

Written by: Brett Lawrence, Esq. On November 12, 2020, Vodafone, the multinational telecommunications company, was fined €12.25 million by Garante, Italy’s data protection authority. The fine is the third largest ordered by the regulator. Garante’s investigation was prompted by hundreds of complaints of unwanted telephone calls by Vodafone promoting its services. The investigation unveiled an information

[Read Full Article](#)

Facebook **Fined \$50,000** **for Violating** **Russian Data** **Localization** **Law**

December 8, 2020

Written by: Brett Lawrence,
Esq. As of 2016, Russia
requires all technology
companies who collect and
process the personal data of
Russian citizens to store that
data on servers located in
Russia. Recently, Russian
authorities discovered that
Facebook was not complying
with this law and
subsequently levied a fine of
4 million ruble (\$53,000)
against the

[Read Full Article](#)

Zoom Settles **Alleged Unfair** **& Deceptive** **Practices with** **Federal Trade** **Commission**

December 8, 2020

HALL BOOTH SMITH, P.C.

Written by: Charles R. Langhorne IV, Esq. In November, the U.S. Federal Trade Commission (the “FTC”) released a Consent Agreement outlining the terms of the settlement the FTC reached with Zoom communications regarding alleged unfair and deceptive practices. The Complaint by the FTC which led to the Consent Agreement, alleged that Zoom mislead users in 3

[Read Full Article](#)

Turkey Places Data Localization Requirement on Social Network Providers

November 10, 2020

Written by: Brett Lawrence, Esq. Last December, we discussed India’s proposed Personal Data Protection Bill and the implications of its data localization requirement. It appears Turkey has now promulgated a similar requirement. Overview On July 29, 2020, Turkey’s legislature, the Turkish Grand

HALL BOOTH SMITH, P.C.

National Assembly, approved the passing of Law No. 5651, an amendment to the country's

[Read Full Article](#)

European Lawsuit Accuses Uber of “Robo- Firing” Drivers

November 10, 2020

Written by: Richard Sheinis, Esq. A lawsuit has been filed with a court in the Netherlands challenging Uber's alleged practice of using automated systems to identify fraudulent activity and terminate drivers based on that process, also known as “Robo-Firing”. This practice, which Uber denies, would potentially violate Article 22 of the GDPR. Article 22 protects data

[Read Full Article](#)

Amazon Subject of Illinois

Biometric Information Privacy Act Lawsuit

November 10, 2020

Written by: Charles R. Langhorne IV, Esq. Recently three plaintiffs filed a class-action lawsuit alleging that Amazon violated Illinois' Biometric Information Privacy Act ("BIPA"), by collecting and storing "voiceprints" without the users' consent. Voiceprints Amazon has a software product called Amazon Connect that companies use to run call-centers. One company with whom Amazon has partnered Pindrop

[Read Full Article](#)

California Privacy Rights Act Passed By California Voters

November 4, 2020

Written by: Rich Sheinis, Esq. and Brett Lawrence, Esq. The votes are in and California's

citizens have spoken, the California Privacy Rights Act (“CPRA”) is now law. Known as CCPA 2.0, CPRA increases the privacy obligations of businesses already subject to the requirements of California’s 2018 California Consumer Privacy Act (“CCPA”). Though not nearly discussed

[Read Full Article](#)

U.S. National Privacy Legislation Introduced: The SAFE DATA Act

October 13, 2020

Written by: Richard Sheinis, Esq. Sen. Roger Wicker, R-Miss., along with three other Republican senators who are members of the Senate Commerce Committee, has introduced yet another national privacy legislation bill, known as the SAFE DATA Act. The full name of the bill is the “Setting an American Framework to Ensure Data Access, Transparency and

[Read Full Article](#)

Facebook **Appeals Order** **from Irish** **Data** **Protection** **Commission**

October 13, 2020

Written by: Charles R. Langhorne IV, Esq. In August 2020, the Irish Data Protection Commission (the “DPC”) issued a preliminary order to Facebook requiring Facebook to suspend data transfers to the U.S. that involve personal data of EU residents. This is the DPC’s first action to enforce the Schrems II ruling issued by the Court

[Read Full Article](#)

H&M Fined for **GDPR** **Violation**

October 13, 2020

Written by: Charles R. Langhorne IV, Esq. On October 1, 2020, the Data Protection Authority of Hamburg (“DPA”), announced a fine of €35.3 million (\$41.3

million) against multinational retail company H&M. The fine is based on excessive monitoring of H&M employees in Germany in violation of GDPR. This is the second-largest fine a single company

[Read Full Article](#)

California's CPRA Is Appearing on Next Month's Election Ballot

October 13, 2020

Written by Brett Lawrence, Esq. Although the upcoming presidential election is currently dominating the political and media discourse, in the data privacy and security world, California's 2020 ballot has been the recipient of much discussion. This is because the California Privacy Rights Act ("CPRA") is on this year's November ballot and can be potentially voted

[Read Full Article](#)

Patient Death

Attributed to Hospital Ransomware Attack

September 23, 2020

Written by: Richard Sheinis, Esq. German authorities are investigating the death of a patient following a ransomware attack on a hospital in Germany. The unknown perpetrators potentially face charges of negligent manslaughter. Last Friday, a patient in need of urgent medical care was re-routed from the Düsseldorf University Hospital, to a hospital more than 30

[Read Full Article](#)

Is the European Hospitality Industry Ready for the Payment Services Directive 2?

September 8, 2020

HALL BOOTH SMITH, P.C.

Written by: Richard Sheinis,
Esq. Many of you are
probably asking what is the
“Payment Services Directive
2 (PSD2)”, before worrying
about being ready for it!
PSD2 is a Directive from the
European Parliament
(Directive (EU) 2015/2366)
intended to modernize
Europe’s payment services
for the benefit of consumers
and business, and to facilitate
innovation, competition, and

[Read Full Article](#)

Update In the Post-Schrems II Era and Guidance for the Use of Standard Contract Clauses

September 8, 2020

Written by: Richard Sheinis,
Esq. It has been almost two
(2) months since the EU Court
of Justice struck down the EU-
US Privacy Shield. At the
same time, while holding that
the Standard Contract
Clauses (“SCC”) in principle
are still valid, the Court

cautioned that SCC must still provide the level of protection guaranteed by the

[Read Full Article](#)

Brazil's LGPD To Take Effect In September

September 8, 2020

Written by: Charles R. Langhorne IV, Esq. In a wild turn of events over a few days at the end of August, Brazil's Lei Geral de Proteção de Dados Pessoais ("LGPD") will take effect on September 16, 2020, barring a presidential veto or another act of the Brazilian legislature. What is the LGPD? The LGPD is

[Read Full Article](#)

CCPA Employee Carve Out Delayed Until 2022

September 8, 2020

Written by: Charles R. Langhorne IV, Esq. Businesses subject to the

HALL BOOTH SMITH, P.C.

California Consumer Privacy Act (“CCPA”) can breathe a small sigh of relief. On August 30, 2020, the California Legislature passed AB 1281. AB 1281 extends the business-to-business and employee personal information carve outs until January 1, 2022. The bill is now headed to the Governor’s

[Read Full Article](#)

2020 **Biometric** **Data Update**

September 8, 2020

Written by: Brett Lawrence, Esq. The utility of biometric data is more prevalent than it has ever been, primarily because developing technology has created a broad swath of convenient uses for it. It can help law enforcement authorities quickly target wanted individuals and also secure a business’ access to proprietary information. The best and most

[Read Full Article](#)

Canada's Supreme Court Addresses Genetic Data Privacy in Split Decision

August 11, 2020

Written by: Charles R. Langhorne IV, Esq. and Brock Wolf Last month, Canada's Supreme Court upheld the constitutionality of provisions of its Genetic Non-discrimination Act ("GNDA") with a 5-4 decision. In 2017, Canada's federal government enacted the GNDA, establishing rules for businesses regarding genetic testing for diseases. Specifically, the GNDA prohibits requiring an individual to undergo

[Read Full Article](#)

EDPB Issues FAQs After Schrems Decision

August 11, 2020

HALL BOOTH SMITH, P.C.

Written by: Charles R. Langhorne IV, Esq. and Brock Wolf Last month, the Court of Justice of the European Union (“CJEU”), Europe’s top court, struck down the EU-US Privacy Shield Framework. The Privacy Shield was created to allow businesses to transfer personal data to the United States from the European Union (“EU”). The decision not

[Read Full Article](#)

Legislation **Introduced to** **Put Limits on** **Use of Facial** **Recognition**

August 10, 2020

Written by: Richard Sheinis, Esq. On August 4, 2020, yet more data privacy legislation was introduced by Senators Bernie Sanders and Jeff Merkley. Titled “The National Biometric Information Privacy Act of 2020,” this continues the trend of law makers introducing piecemeal, and frequently punitive, data privacy legislation rather than working on a single comprehensive data

[Read Full Article](#)

Early CCPA Litigation is Underway as Walmart Faces Class Action Lawsuit

August 9, 2020

Written by: Brett Lawrence, Esq. and Brock Wolf Early last month, Walmart joined Minted Inc., Zoom, TikTok, and Salesforce.com to become the largest company targeted by a class action lawsuit following a data breach under the California Consumer Privacy Act (“CCPA”). On July 10, 2020, shortly after CCPA enforcement began on July 1, Lavarious Gardiner

[Read Full Article](#)

EU High Court Invalidates EU-US Privacy Shield Framework

July 16, 2020

HALL BOOTH SMITH, P.C.

Written by: Brett Lawrence, Esq. On July 16, 2020, the Court of Justice of the European Union (“CJEU”), Europe’s top court, struck down the EU-US Privacy Shield Framework. The Privacy Shield was created to allow businesses to transfer personal data to the United States from the European Union (“EU”). The CJEU premised its decision invalidating

[Read Full Article](#)

China **Publishes** **Draft Data** **Security Law**

July 14, 2020

Written by: Brett Lawrence, Esq. and Brock Wolf After deliberating a draft Data Security Law from June 28 to June 30, 2020, China’s Standing Committee of the National People’s Congress (“NPC”) published the draft law on July 2, 2020. The draft law calls for China to develop a “standard, interconnected and interactive, secure and controllable”

[Read Full Article](#)

South Africa's Data Privacy Law Is Now In Effect

July 14, 2020

Written by: Charles R. Langhorne IV, Esq. South Africa's newest data privacy law, the Protection of Personal Information Act ("PoPIA") is now in effect. There is a 12-month grace period, and enforcement will not begin until July 1, 2021. The PoPIA applies to businesses that process personal information in South Africa, whether or not they

[**Read Full Article**](#)

Congress is All Talk And No Action When It Comes To Data Privacy

June 30, 2020

Written by: Richard Sheinis, Esq. In the last fifteen (15) months, no less than six (6) data privacy Bills have been introduced in the Senate. Two of these Bills are

specifically related to data collection and use in response to COVID-19. This does not include the Data Accountability and Transparency Act of 2020, announced by

[Read Full Article](#)

[**CPRA to Appear on California's November 2020 Election Ballot**](#)

June 27, 2020

Written by: Brett Lawrence, Esq. As businesses continue to prepare for the enforcement of the California Consumer Privacy Act ("CCPA"), which will begin on July 1, 2020, new privacy legislation is already on the way. On June 24, 2020, the Office of the Secretary of State of California announced that the California Privacy Rights Act

[Read Full Article](#)

[**Thailand**](#)

Delays Data Protection Law Because of COVID-19

June 9, 2020

Written by: Richard Sheinis,
Esq. Thailand's Personal Data
Protection Act was passed in
May 2019, and was scheduled
to go into effect May 27,
2020. The Act is very similar
to the European Union's
General Data Protection
Regulation. Only a few days
before the Act was to become
effective, it was decided that
22 types

[Read Full Article](#)

EDPB Issues Statement on Hungary's Decree to Suspend Rights Bestowed to Data Subjects Under the GDPR

June 9, 2020

HALL BOOTH SMITH, P.C.

Written by: Brett Lawrence,
Esq. On May 4, 2020,
Hungary issued a
governmental decree
suspending the rights of data
subjects under Articles 15 to
22 of the General Data
Protection Regulation
("GDPR") in an attempt to
contain the spread of the
COVID-19 pandemic. Such
articles include giving
individuals, whose personal
data has been collected, the

[Read Full Article](#)

Brazilian **LGPD** **Effective and** **Enforcement** **Dates in Flux**

June 9, 2020

Written by: Charles R.
Langhorne IV, Esq. Brazil's
new data privacy law, the
"LGPD," was set to go into
effect on August 15, 2020.
The LGPD is based largely on
the European Union's GDPR.
Due to the impact COVID-19
has had on businesses, the
effective and enforcement
dates have been delayed.
Keeping track of the

[Read Full Article](#)

Dutch Court Goes Too Far In Enforcing Privacy Regulation

June 2, 2020

Written by: Richard Sheinis, Esq. A Dutch court has ruled that a grandmother is violating the EU's General Data Protection Regulation by posting photographs of her grandchildren on her social media account without the consent of the children's parents. The court's ruling arose from a complaint filed by the children's mother, who wanted the photographs

[**Read Full Article**](#)

Washington D.C. Amends Data Breach Notification Statute

May 27, 2020

Written by: Charles R. Langhorne IV, Esq.
Washington D.C. amended its data breach notification

statute at the end of March.
The new law is set to take effect by June 13, 2020. This is the first update to the law since it was passed in 2007. Personal Information Defined Washington D.C. is following the national

[Read Full Article](#)

HHS Reduces Enforcement of HIPAA Violations for COVID-19 Community Based Testing Sites

May 21, 2020

Written by: Brett Lawrence, Esq. On April 14, 2020, The Department of Health and Human Services (“HHS”) Office of Civil Rights (“OCR”) announced it will exercise further enforcement discretion in easing back penalties for failing to comply with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The enforcement discretion has retroactive effect beginning

[Read Full Article](#)

European Data Protection Board Calls Out Adtech Industry Over Cookie Consent Practices

May 12, 2020

Written by: Charles R. Langhorne, IV, Esq. As we continue to wait for the ePrivacy Regulation, the European Union is being left to govern cookie consent procedures on their own. Some individual member states are taking it upon themselves to issue guidance, while others sit back and wait. I wrote an article late last year outlining

[Read Full Article](#)

CCPA 2.0 May Be On the November Ballot

May 12, 2020

Written by: Charles R.

HALL BOOTH SMITH, P.C.

Langhorne, IV, Esq. The California Consumer Privacy Act (“CCPA”) is not set to be enforced until at least July, but just last week the group that spearheaded the CCPA ballot initiative in 2018 has submitted 900,000 signatures to put a new initiative, the California Privacy Rights Act (“CPRA”) on the November

[Read Full Article](#)

European Data Protection Board Issues Guidelines On The Use of Location Data and Contact Tracing Tools In the Context of COVID-19

May 12, 2020

Written by: Richard Sheinis, Esq. Unlike the United States, where Senators are first introducing legislation to deal with the use of personal information in the context of COVID-19, the European Data Protection Board (“EDPB”) relies on established

legislation to govern the use of location data and contact tracing tools. (Hint: the U.S. needs to pass

[Read Full Article](#)

[Senators Introduce Bill to Protect Personal Data Amidst COVID-19](#)

May 12, 2020

Written by: Richard Sheinis, Esq. On April 30, 2020, Republican Senators Wicker (MS), Thune (SD), Moran (KS) and Blackburn (TN), announced the introduction of the “COVID-19 Consumer Data Protection Act,” intended to protect health, geolocation and proximity data. These types of personal data are related to contact tracing, the process of identifying persons with whom

[Read Full Article](#)

[Are Countries](#)

Willing To **Bend The** **Privacy Rules** **To Track** **COVID-19**

April 14, 2020

Written by: Richard Sheinis, Esq. Many countries are using geolocation data from phones to track COVID-19. Singapore, the United Kingdom and Israel have developed their own apps for tracking people's movements. In Europe, mobile phone companies such as Vodafone, have agreed to share location data. The European Data Protection Board has appointed a group of

[**Read Full Article**](#)

New York's **S.H.I.E.L.D.** **Act Is Here**

April 13, 2020

Written by: Charles R. Langhorne IV, Esq. The COVID-19 world that we are living in is has changed the perspective of many

HALL BOOTH SMITH, P.C.

businesses from proactive to reactive. Businesses (rightly so) are concerned with making payroll so that their employees can continue to pay their mortgages as opposed to preparing the company for impending data privacy

[Read Full Article](#)

Security Advice for Zoom Videoconferen cing

April 13, 2020

Written by: Sean Cox, Esq.
The COVID-19 pandemic and the widespread shelter in place orders have, temporarily at least, changed how humans interact. Luckily, there are more options today than ever before which allow many to maintain a modicum of normalcy. Companies, schools, churches, families, and friends have turned to video conferencing solutions to stay

[Read Full Article](#)

California **Attorney** **General** **Fiddles While** **Rome Burns**

March 30, 2020

Written by: Richard Sheinis, Esq. On March 17 a coalition of 35 advertising groups sent California Attorney General Xavier Becerra a letter calling for a delay in the enforcement of the California Consumer Privacy Act (“CCPA”) because of COVID-19. Enforcement of the CCPA is currently scheduled to begin July 1. The Attorney General’s office refused

[Read Full Article](#)

HHS Releases **Bulletin** **Waiving** **Certain** **Provisions of** **HIPAA**

March 19, 2020

Written by: Chase Langhorne, Esq. The U.S. Department of

HALL BOOTH SMITH, P.C.

Health and Human Services (“HHS”) released a bulletin this week waiving sanctions and penalties as of March 15, 2020 for non-compliance with certain provisions of HIPAA. The waiver centers around allowing people on the front lines to adequately handle and manage COVID-19 cases. Specifically, HHS is

[Read Full Article](#)

CROATIA’S **ATTEMPT TO** **BREAK THE** **ePRIVACY** **REGULATION** **STALEMATE**

March 10, 2020

Written by: Chase Langhorne, Esq. On February 21, 2020, Croatia released its proposal to attempt to move the ePrivacy Regulation across the finish line. The ePrivacy Regulation was proposed in 2017 with the main purpose of regulating personal data as it relates to internet cookies. The initial plan was for it to pass at the same

[Read Full Article](#)

Egypt Passes **Personal Data** **Protection** **Law**

March 10, 2020

On February 24, 2020, Egypt's Parliament passed the Personal Data Protection Law ("PDPL"). The law has many similarities to the European Union's General Data Protection Regulation ("GDPR"). Scope The PDPL applies to Egyptian citizens and non-Egyptian citizens residing in Egypt. This is similar to GDPR, but slightly more limiting because GDPR applies to any person

[**Read Full Article**](#)

"SALE" **UNDER THE** **CCPA**

March 10, 2020

Written by: Sean Cox, Esq.
The California Consumer Privacy Act of 2018 ("CCPA") officially went into effect on January 1, 2020. According to the California Attorney General, enforcement will begin on July 1, 2020. One of

the most important provisions of the CCPA allows consumers to opt-out of the sale of their personal information. Among

[Read Full Article](#)

We All Know About GDPR's Right to Erasure, Does This Mean You Have to Delete Data From Backups As Well?

March 10, 2020

Written by: Richard Sheinis, Esq. In this business, we are all familiar with GDPR's right to erasure (commonly called "the right to be forgotten") granted by the GDPR. The question that often comes up is when a data subject exercises their right to erasure, does the organization also have to erase the data subject's personal

[Read Full Article](#)

Brexit Is Here, so What Does That Mean for Data Privacy?

February 13, 2020

Written by: Richard Sheinis, Esq. Now that the UK has a withdrawal agreement with the EU, what will this mean for data privacy for personal data in the UK, as well as for personal data that is transferred between the UK and other countries. UK's Information Commissioner's Office ("ICO") has provided some answers. For the

[**Read Full Article**](#)

The Irish DPA Has Opened Investigations Into Google and Tinder

February 13, 2020

Written by: Chase Langhorne, Esq. Ireland's Data Protection Commission (DPC) has opened two separate investigations into Google and Tinder, respectively, for GDPR violations. Google The

HALL BOOTH SMITH, P.C.

investigation into Google centers around how Google treats location data collected from end users. “The Inquiry will set out to establish whether Google has a valid legal basis for processing

[Read Full Article](#)

CA Attorney General Issues New Draft of CCPA Regulations

February 13, 2020

Written by: Richard Sheinis, Esq. On February 7, 2020 the California Attorney General published a “redline” version of the CCPA Regulations. These regulations are open for public comment until February 24, 2020. In the meantime, here are a few of the more important redline changes in the latest draft: The definition of household is clarified

[Read Full Article](#)

Australia Finalizes

Consumer Data Rights Rules

February 13, 2020

Written by: Chase Langhorne,
Esq. On November 26, 2017
Australia introduced the
consumer data right (CDR)
which was designed to give
consumers greater control
over their personal data.
Since that time, Australians
have been waiting for the
Australian Competition and
Consumer Commission
(ACCC) to issue rules
governing exactly how a
consumer will be able to

[**Read Full Article**](#)

State Data Breach Notification Updates

January 14, 2020

Written by: Chase Langhorne,
Esq. Starting on January 1,
2020 amendments to data
breach notification statutes in
Illinois, Oregon, and Texas
take effect. Illinois The
Personal Information
Protection Act ("PIPA")

requires public and private entities that handle non-public personal information to notify affected Illinois residents following a data breach. An amendment now requires public and

[Read Full Article](#)

Georgia Data Breach Class Action

January 14, 2020

Written by: Sean Cox, Esq. On December 23, 2019, in a case of first impression, a unanimous Georgia Supreme Court reversed the trial court and Court of Appeals in a putative data breach class action, holding that there were sufficient allegations of a legally cognizable injury to survive a motion to dismiss. The case arose out

[Read Full Article](#)

New Rules in China to Prevent the Illegal

Collection of Personal Information By Mobile Apps

January 14, 2020

Written by: Richard Sheinis, Esq. Over the past year, Chinese regulators have sought to crack down on the collection and use of personal data by mobile apps. New regulations published jointly by China's Cyberspace Administration, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration for Market Regulation, address the illegal collection

[**Read Full Article**](#)

Doorstep Dispensaree Gets UK Fine for GDPR Violations

January 14, 2020

Written by: Richard Sheinis, Esq. Doorstep Dispensaree, a

London-based pharmacy which supplies medicine to individuals and care homes, left approximately 500,000 documents in unlocked containers stored in a courtyard at one of its premises. Documents contained personal data including names, addresses, dates of birth, medical and prescription information. The documents were not secure, and the

[Read Full Article](#)

The e-Privacy Regulation Strikes Out Again

December 10, 2019

Written by: Richard Sheinis, Esq. The e-Privacy Regulation, which was supposed to be a close cousin to the General Data Protection Regulation, was first proposed by the European Commission in January 2017. However, here we are nearly 3 years later, and the latest draft of the e-Privacy Regulation was once again been rejected by the

[Read Full Article](#)

Another Attempt at Federal Privacy Legislation

December 10, 2019

Written by: Richard Sheinis,
Esq. In yet another attempt to
pass federal privacy
legislation, on November 26,
U.S. Senator Maria Cantwell,
D-Wash., introduced the
Consumer Online Privacy
Rights Act (“COPRA”). COPRA
would apply to information
that identifies or is
reasonably linked to an
individual residing in the U.S.
or a consumer device.
COPRA would generally

[Read Full Article](#)

India’s Data Protection Law Takes a Step Forward

December 10, 2019

Written by: Chase Langhorne,
Esq. In an ever-increasing
data driven world, India’s
proposed Personal Data
Protection Bill (“PDPB”) took a

step forward on December 4th when the Indian Prime Minister Narendra Modi approved the bill for tabling in parliament. The PDPB was first proposed in 2018 and is designed to protect the personal data of

[Read Full Article](#)

Singapore **Takes Next** **Steps Towards** **Updating Its** **Data** **Protection** **Law**

December 10, 2019

Written by: Chase Langhorne, Esq. In May 2019 Singapore's data protection authority, the Personal Data Protection Commission ("PDPC") took steps to update its existing data protection legislation, the Personal Data Protection Act (2012). The PDPC issued a statement regarding their progress and introduced new data breach notification procedures that are expected to be a part

[Read Full Article](#)

California DMV Sells Personal Information

December 10, 2019

Written by: Chase Langhorne, Esq. A recent public records request to the California DMV shows that the California DMV is selling personal information drivers provide to receive a driver's license to private companies to the tune of roughly \$50 million per year. The reasoning provided by a representative of the California DMV is that "nformation

[**Read Full Article**](#)

Cookies - The Need For Regulation

November 12, 2019

Written by: Chase Langhorne, Esq. While we await the completion of the ePrivacy Regulation, countries are taking matters into their own hands by both publishing guidance and issuing fines related to cookie consent mechanisms on websites. The

existing ePrivacy Directive was published in 2009. Upon the passage of GDPR in 2018, an updated ePrivacy Regulation

[Read Full Article](#)

EU Investigations into Microsoft

November 12, 2019

Written by: Chase Langhorne, Esq. On October 21, the European Data Protection Supervisor (“EDPS”) issued an update on its investigation that began in April 2019 into contracts between Microsoft and EU institutions. “EU institutions” are comprised of the following seven decision making bodies of the EU: the European Parliament, the European Council, the Council of

[Read Full Article](#)

Fighting Fire With Fire: Legal And Ethical Issues

of Active Defense and Hacking Back

November 12, 2019

Written by: Sean Cox, Esq.
When a company is hacked, an immediate thought is sometimes whether they can hack back. The next question is then, "Can we do that?" Hacking back describes striking back at the cyber criminal by accessing, damaging, or breaching the criminal's own system. The reasons for hacking back can be several:

[**Read Full Article**](#)

Facial Recognition Technology and GDPR Compliance

November 12, 2019

Written by: Richard Sheinis, Esq. A soccer team in Denmark is using facial recognition technology to stop unruly fans, apparently with the approval of the Danish Data Protection

HALL BOOTH SMITH, P.C.

Agency (“DDPA”). The technology is used to scan fans as they enter the stadium. The scans are then compared against a list of banned troublemakers to determine

[Read Full Article](#)

Country of Georgia Hit by Massive Cyber Attack

November 12, 2019

Written by: Richard Sheinis, Esq. More than 2,000 websites, including court websites and the national TV station, were knocked out by a massive cyber attack in the country of Georgia. A state sponsored political attack is suspected as many of the website home pages were replaced with an image of former President Mikheil Saakashvili and the

[Read Full Article](#)

Singapore’s Privacy Watchdog

Issues Two **Fines**

November 12, 2019

Written by: Richard Sheinis, Esq. Singapore's Personal Data Protection Commission ("PDPC") has assessed two large fines against companies for data breaches. The telecommunications company, Tingteltel, has been fined \$25,000 for a data breach involving its My Singtel mobile app. A problem in the design of the mobile app allowed My Singtel users to potentially access

[**Read Full Article**](#)

U.S. Federal **Legislation on** **Data Privacy** **Unlikely This** **Year**

October 7, 2019

Written by: Richard Sheinis, Esq. With the California Consumer Privacy Act ("CCPA") ready to go into effect in 2020, and other states lined up to follow with similar legislation, there has

been a greater push for a federal privacy law. Unless there is a federal privacy law that supersedes state law, businesses will be in

[Read Full Article](#)

German Data Protection Authorities Releases a New Model to Calculate FDPR Fines

October 7, 2019

Written by: Richard Sheinis, Esq. German data protection authorities have published a new model for calculating fines under GDPR, which, is likely to lead to higher fines. While this model is strictly being tested in Germany, since GDPR should be applied equally across the EU, it is possible that this model could be expanded to

[Read Full Article](#)

The Court of Justice of the

European Union Issues a Ruling on Cookie Consent Requirements

October 7, 2019

Written by: Rich Sheinis, Esq.
On October 1, 2019, the CJEU issued a ruling establishing that consent to use cookies cannot be validly obtained through a pre-checked box. In this particular case, an online gaming company, Planet49 GmbH, had a lottery which required internet users to provide personal data. The web page contained a pre-ticked

[**Read Full Article**](#)

Ecuador Data Breach

October 7, 2019

Written by: Chase Langhorne, Esq. On September 16th the State Attorney General's Office of Ecuador released a statement (Spanish) indicating that a privacy breach concerning the

personal data of Ecuadorian citizens was being investigated. Specifically, servers belonging to Novaestrat, an Ecuadorian data analytics company. The breach was first discovered by the ethical-hacking group vpnMentor. Further

[Read Full Article](#)

The Court of Justice of the European Union Issues a Ruling on the Right to be Forgotten

October 7, 2019

Written by: Chase Langhorne, Esq. On September 24 the Court of Justice of the European Union (CJEU) issued a landmark ruling on GDPR's "right to be forgotten." The case was brought by Google challenging an order, and subsequent fine, issued by the French Data Protection Authority (CNIL), over Google's choice not to comply with CNIL's

[Read Full Article](#)

EUROPEAN DATA PROTECTION BOARD ISSUES DRAFT GUIDANCE ON THE PROCESSING OF PERSONAL DATA THROUGH VIDEO DEVICES

September 11, 2019

Written by: Richard Sheinis,
Esq. The European Data
Protection Board (“EDPB”)
recently issued guidance on
the use of video devices to
process personal data. The
guidelines are in draft form,
and were open for public
comment through September
9, 2019. The final version of
the guidelines is expected
later this year. The use of
video

[Read Full Article](#)

Portugal's GDPR Law is Now in Effect

September 10, 2019

Written by: Chase Langhorne, Esq. On August 8, Portugal's long-awaited data protection law went into effect. The legislation was originally passed in June, but awaited Presidential signature and publication in the Official Journal. The official name of the legislation is known as "Lei de Execução do Regulamento Geral sobre a Proteção de Dados" (English translation:

[Read Full Article](#)

CAYMAN ISLANDS DATA PROTECTION LAW GOES INTO EFFECT SEPTEMBER 30, 2019

September 10, 2019

Written by: Richard Sheinis, Esq. The Data Protection Law,

2017, (“DPL”) introduces globally-recognized principles surrounding the use of personal information to the Cayman Islands. Similar to the GDPR and other data privacy legislation, individuals will have several data access rights. These rights include the right to be informed, the right to access their data, the

[Read Full Article](#)

Ransomware **on the Rise**

August 21, 2019

Written by: Chase Langhorne, Esq. Ransomware attacks are plaguing businesses all over the world and, unfortunately, show no signs of slowing down. The scenario goes something like this: you come into work, pour a cup of coffee, go to check your email and nothing seems to work. You cannot open your email, nor any files

[Read Full Article](#)

EU Court of **Justice Rules** **Using**

Facebook's **"Like" Button** **Creates a Joint** **Data** **Controller** **Relationship**

August 13, 2019

Written by: Richard Sheinis,
Esq. Fashion ID is an online
retailer whose website used a
plug-in to feature a Facebook
"Like" button. As a result of
the plug-in, when a user lands
on Fashion ID's website,
information about the user's
IP address and browser string
is automatically transferred to
Facebook. This transfer of
information occurs

[Read Full Article](#)

Class Action **Proceeds** **Against** **Facebook for** **Violation of** **Illinois** **Biometric** **Information**

Privacy Act **("BIPA")**

August 13, 2019

Written by: Richard Sheinis, Esq. The Ninth Circuit has ruled that a case against Facebook for violating the Illinois Biometric Information Privacy Act can proceed as a class action. The lawsuit stems out of Facebook's "Tag Suggestions" feature. When a Facebook user enables the Tag Suggestions feature, Facebook uses facial recognition technology to analyze whether

[Read Full Article](#)

German DPA **Tackles** **Artificial** **Intelligence**

August 13, 2019

Written by: Chase Langhorne, Esq. Artificial Intelligence ("AI") devices can make everyday life easier. They can tell us the temperature outside, set a timer, and even order a pizza; but what is happening to all the data being collected by these devices? Think of everything

an AI device hears in your
living room while waiting

[Read Full Article](#)

[Arkansas's New Breach Reporting Requirements Go Into Effect This Month](#)

July 3, 2019

Written by: Anthony E. Stewart, Esq. Earlier this year, Arkansas Governor Asa Hutchinson signed HB 1943, which amends the Personal Information Protection Act. It goes into effect on July 23, 2019. The new law expands the definition of 'personal information,' imposes additional reporting obligations, and enacts specific retention requirements. It continues to apply to any

[Read Full Article](#)

[Nevada's New Privacy Law Goes Into](#)

Effect in October

June 27, 2019

Written by: Anthony E. Stewart, Esq. Does your business have a website? If so, it will likely need to comply with yet another new online privacy law that goes into effect in a little over three short months. Nevada recently passed SB220, which amends its existing online privacy law and provides Nevada residents the ability,

[Read Full Article](#)

Maine Enacts Internet Privacy Legislation to Go Into Effect Next Year

June 18, 2019

Written by: Anthony E. Stewart, Esq. California and New York are not the only states making waves in the world of technology and privacy. Earlier this month, Governor Janet Mills of Maine signed into law one of the

nation's strictest internet
privacy protection bills – An
Act To Protect the Privacy of
Online Customer Information.

[Read Full Article](#)

Why Businesses Throughout The Country Should Be Worried About New York's SHIELD Act

June 17, 2019

Written by: Richard Sheinis,
Esq. New York's SHIELD Act
has passed the New York
Senate, and now awaits
passage in the Assembly
before it goes to the Governor
to sign into law. While the
Act contains new rules
regarding data breaches and
data breach notification,
businesses should be most
concerned about the
increased geographic
coverage

[Read Full Article](#)

India's Controversial Personal Data Protection Bill, If Passed, Goes Into Effect in 2020

June 5, 2019

Written by: Anthony E. Stewart, Esq. India's draft privacy law, Personal Data Protection Bill, 2018, is an important step as India moves toward a digital economy; however, it is one of the more controversial privacy laws amongst privacy experts. Critics have accused India Prime Minister Narendra Modi's Bharatiya Janata Party of creating a "surveillance state"

[Read Full Article](#)

GDPR: A Year in Review and the Need for Clarity

June 5, 2019

As the first year of GDPR's governance comes to a close,

the hysteria has subsided, but the reality of the reach of GDPR is all the more real. Since its May 25, 2018 effective date European State Data Protection Authorities (“DPA”) have received more than 64,000 data breach notifications. Those 64,000 notifications have resulted in more

[Read Full Article](#)

California **Consumer** **Privacy Act of** **2018**

June 5, 2019

Written by: Chase Langhorne, Esq. It may come as a surprise, but only 11 states have constitutional provisions that contain an explicit right to privacy. Specifically, California voters amended their state constitution to include the right of privacy among the inalienable rights of all people in 1972. In 2018, the California legislature passed the California

[Read Full Article](#)

Scam Alert: **Virtual** **Kidnappings** **Are on the** **Rise**

May 20, 2019

Written by: Anthony E. Stewart, Esq. Your cell phone rings. You look down, and to your delight, it's your daughter. She's in college now and remembering to 'give mom a call every once in a while' seems to be an impossible task. You quickly answer, and your delight immediately turns to terror: "We have your daughter,"

[**Read Full Article**](#)

HIPAA **Breaches** **Reported to** **HHS During** **the First** **Quarter of** **2019**

April 24, 2019

Atlanta attorney Anthony Stewart created this graphic that reflects the summary of

the HIPAA breaches that were reported to the U.S. Department of Health and Human Services during the first quarter of 2019.

[Read Full Article](#)

Pennsylvania **Court Holds** **Employer** **Liable For** **Breach Of** **Employees'** **Personal** **Information**

December 6, 2018

Written by: Richard Sheinis, Esq. In a recent case, Dittman v. The University of Pittsburgh Medical Center, the Pennsylvania Supreme Court found that the Medical Center owed a duty to their employees to exercise reasonable care in collecting and storing their personal and financial information on its computer systems. Many other courts around the country have

[Read Full Article](#)

Canada's Breach Notification Rules Go Into Effect Nov. 1

October 31, 2018

Written by: Anthony E. Stewart, Esq. Any organization subject to Canada's Personal Information Protection and Electronic Document Act (PIPEDA) will have new data breach notification rules to follow starting tomorrow. This change will affect businesses of all sizes and may affect U.S. companies that process Canadians' personal information even if their operations are solely on the

[**Read Full Article**](#)

Brazil's General Data Privacy Law Goes Into Effect in 2020

October 10, 2018

Written by: Anthony E. Stewart, Esq. Brazil is one of

the latest countries to implement comprehensive data privacy regulation. Brazilian President Michel Temer recently signed into law the General Law of Protection of Personal Data, which goes into effect in February, 2020. The new law imposes detailed rules for the collection, processing, and storage of personal data,

[Read Full Article](#)

Dangerous **Phishing Scam** **Targeting** **Employees'** **Direct Payroll** **Deposits**

September 27, 2018

Written by: Anthony E. Stewart, Esq. The Federal Bureau of Investigations (FBI) has issued a warning about a phishing scam that is targeting employees who receive their paychecks by direct deposit. Cybercriminals are targeting the online payroll accounts of employees around the country in a variety of industries, especially those in education, healthcare, and

commercial aviation. Here's
how

[Read Full Article](#)

HHS Issues Guidance on Disposing of Electronic Devices and Media with Personal Data

August 15, 2018

Written by: Anthony E.
Stewart, Esq. The U.S.
Department of Health and
Human Services Office for
Civil Rights (OCR) has
issued guidance for disposing
of technology that contains
sensitive information, such as
financial or protected health
information. While the OCR's
intended audience is limited
to covered entities and
business associates subject to
HIPAA, all organizations that
store or

[Read Full Article](#)

Georgia Court of Appeals

Makes First Foray Into Standing in Data Breach Suits

August 10, 2018

Written by: Sean Cox, Esq. On June 26, 2017, the Georgia Court of Appeals issued an opinion in Collins, et al. v. Athens Orthopedic Clinic, A18A0296. This is the first Georgia appellate decision squarely addressing the issue of standing in a data breach case. Since the United States Supreme Court decision in Spokeo, Inc. v. Robins, 578 U.S. ____

[Read Full Article](#)

OCR Issues Guidance on Software Vulnerabilities and Patching

August 1, 2018

Written by: Anthony E. Stewart, Esq. Last month, the U.S. Department of Health and Human Services Office

for Civil Rights (OCR) provided guidance regarding software vulnerabilities and patching. In simple terms, a software vulnerability is a weakness, design or implementation error that can lead to an unexpected and undesirable event, compromising the security of a system. After a

[Read Full Article](#)

Wave of **“GDPR like”** **Data Privacy** **Legislation** **continues with** **California’s** **Sweeping New** **Data Privacy** **Law**

July 2, 2018

Written by: Richard Sheinis, Esq. On June 28, 2018 California legislators enacted the California Consumer Privacy Act of 2018, granting new protections for consumers’ online data. The law does not take effect until January 1, 2020. It can still be amended by the California Legislature prior to that date,

HALL BOOTH SMITH, P.C.

but don't expect too much to
change

[Read Full Article](#)

GDPR Wave Hits the U.S.

June 25, 2018

Written by: Rich Sheinis, Esq.
The wave of data protection
that is the EU General Data
Protection Regulation
("GDPR") has hit the shores
of the U.S. with states
passing GDPR look-a-like
legislation. All 50 states have
data breach notification
statutes, which require
notification of affected
individuals after a breach.
The new trend, following the
lead of GDPR, is

[Read Full Article](#)

Dangerous Phishing Scam Targeting Employers This Tax Season

January 31, 2018

Written by: Anthony E.
Stewart, Esq. The Internal

HALL BOOTH SMITH, P.C.

Revenue Service (IRS) and state tax agencies are warning employers about one of the most dangerous phishing scams in the tax community. Cybercriminals are targeting organizations nationwide and tricking payroll personnel into disclosing the sensitive personal information of an organization's entire workforce. Last year, more than 200 employers

[Read Full Article](#)

North Carolina Introduces New Data Breach Legislation

January 24, 2018

Written by: Richard Sheinis, Esq. On January 8, 2018, North Carolina Attorney General Josh Stein, and State Representative Jason Saine, proposed new data breach legislation entitled, "Act to Strengthen Identity Theft Protections" to update the current North Carolina data breach law. This legislation is in response to the recent data breaches at Equifax and Uber, the

[Read Full Article](#)

Cyber Attack Quick- Response Checklist for HIPAA Covered Entities

August 29, 2017

Written by: Anthony E. Stewart, Esq. Ransomware attacks, like other cyber-attacks, are occurring more and more frequently, and healthcare entities are common targets. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) has issued a quick-response checklist and infographic detailing steps a HIPAA covered entity or its business associate should take to respond to a cyber-related

[Read Full Article](#)

PART 2: The European Union's

General Data Protection Regulation: Two Important Steps to Take

August 15, 2017

Featured on Hospitality Upgrade Magazine's Tech Talk. Written by: Sam Crochet, Esq. In my June column, we discussed why the General Data Protection Regulation (GDPR) matters to the hospitality industry and the technical/organizational steps members should take to comply with the regulation. Practically speaking, any U.S. company desirous of European customers must comply with the GDPR as of May

[Read Full Article](#)

The European Union's General Data Protection Regulation: What Steps

Must Members of the Hospitality Industry Take?

July 14, 2017

Featured on Hospitality Upgrade Magazine's Tech Talk. Written by: Sam Crochet, Esq. US companies collect, analyze, and leverage consumer data to optimize efficiency, advertise and, hopefully, increase profits. However, with the rise of data breach incidents, varying laws and consumer demand pressure companies to secure networks, scrutinize vendor usage—such as security of one cloud processor versus another, and

[Read Full Article](#)

Advice on Selecting a Data Protection Officer

April 6, 2017

Written by: Sean Cox, Esq.
Having a single person responsible for a company's

data privacy and security has long been good business practice, but for many it will soon be a legal requirement. The GDPR requires that organizations under its auspices appoint a Data Protection Officer (“DPO”). These requirements apply to more than just companies located

[Read Full Article](#)

4th Circuit **Severely** **Limits Data** **Breach** **Lawsuits**

April 6, 2017

Written by: Sean Cox, Esq. A recent decision from the Federal 4th Circuit Court of Appeals is likely to make it much harder for plaintiffs within its borders bringing lawsuits following a data breach. In *Beck v. McDonald*¹, the 4th Circuit Court of Appeals held that allegations of enhanced risk of future identity theft following a data

[Read Full Article](#)

Data Breach **Plaintiffs Find** **New Ways** **Around** **Landmark** **Supreme** **Court Decision**

February 17, 2017

Written by: Sam Crochet, Esq.
In-house counsels are facing growing pressure to perform risk assessments and address internal policies to avoid data breaches for a new reason (as if they needed one). Data breach plaintiffs, depending on the state, may now find their cases welcome in state courts despite struggling to prove a clear “injury” in

[Read Full Article](#)

Failure To **Learn From** **Own Mistakes** **Leads To \$3.2** **Million HIPAA** **Penalty**

February 13, 2017

Written by: Richard Sheinis,

HALL BOOTH SMITH, P.C.

Esq. A mistake is nothing more than an opportunity to learn. Of course, you have to take advantage of that opportunity. Children's Medical Center of Dallas failure to take that opportunity has led to a HIPAA civil monetary penalty of \$3.2 million. In 2010, Children's filed a report with OCR indicating the

[Read Full Article](#)

FTC Fines **VIZIO \$2.2** **Million For** **Collecting** **Viewer Data** **Without** **Consent**

February 7, 2017

Written by: Richard Sheinis, Esq. Vizio, Inc., one of the world's largest manufacturers of internet connected televisions has agreed to pay \$2.2 million to settle charges by the Federal Trade Commission and the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without the consumers'

[Read Full Article](#)

OCR Gives Another Expensive Lesson in HIPAA Security Compliance

January 23, 2017

Written by: Richard Sheinis,
Esq. The U.S. Department of
Health and Human Services,
Office of Civil Rights (“OCR”)
has agreed to a \$2.2 million
settlement with MAPFRE Life
Insurance Company of Puerto
Rico for potential non-
compliance with the HIPAA
Security Rule. MAPFRE filed a
report with HHS stating a
“pen drive” containing ePHI
of 2,209 individuals

[Read Full Article](#)

Medical Provider To Pay \$475,000 For Failing To Timely Report

The Loss Of PHI

January 13, 2017

Written by: Richard Sheinis, Esq. The importance of timely reporting breaches of Protected Health Information (“PHI”) is now underscored by the U.S. Department of Health and Human Services (“HHS”) first ever enforcement action against a medical provider for failing to timely report a breach. Presence Health, a health care network with approximately 150 locations, including hospitals,

[**Read Full Article**](#)

Court Dismisses Shareholder Derivative Suit Over 2014 Home Depot Breach

December 6, 2016

Written by: Richard Sheinis, Esq. An Atlanta court has dismissed a shareholder derivative suit against Home

HALL BOOTH SMITH, P.C.

Depot's CEO and Board Chairman, Executive Vice-President and Chief Information Officer, and several members of the Board of Directors, arising from the 2014 breach which affected the credit card data of 56 million customers. The suit by Home Depot shareholders

[Read Full Article](#)

UMass To Pay \$650,000 For HIPAA Violations

November 30, 2016

Written by: Richard Sheinis, Esq. The University of Massachusetts Amherst is paying \$650,000 to OCR to settle allegations of HIPAA violations that occurred in 2013. UMass neglected to designate their Center for Language, Speech and Hearing as a health care component (Oops!), and neglected to have the most basic electronic security in place, including a firewall.

[Read Full Article](#)

Minnesota Pacemaker Manufacturer Faces Class Action for Cyberattack Risks

September 1, 2016

Written by: Sam Crochet, Esq.
St. Jude Medical Inc., a producer of remote-access pacemakers and implantable defibrillators, is under intense scrutiny for what cybersecurity researchers have deemed a negligent risk of attack. A California patient has filed a federal class action suit alleging the manufacturer failed to provide adequate cybersecurity controls for its implants. St. Jude

[Read Full Article](#)

Home Depot Gets Nailed with \$7.5 Million in Legal Fees In

Data Breach **Class Action**

August 25, 2016

Written by: Tiffany Winks,
Esq. On Tuesday, August 23,
2016, a Federal Judge in
Atlanta awarded a whopping
\$7.5 million in legal fees to
consumers' lawyers in a
lawsuit against Home Depot
for its 2014 data breach. Not
only did the Court award
these substantial attorney's
fees, but it also tipped its hat
to the lawyers

[Read Full Article](#)

Court of **Appeals** **Affirms** **Dismissal of** **Class Action** **Data Breach** **Case**

August 15, 2016

Written by: Richard Sheinis,
Esq. The Georgia Court of
Appeals recently held the line
against data breach cases
when it affirmed the dismissal
of a class action against the
Georgia Department of

HALL BOOTH SMITH, P.C.

Labor.1) Thomas McConnell had filed a class action against the Georgia Department of Labor after a department employee sent a spreadsheet with the name, Social

[Read Full Article](#)

Third Circuit Court of Appeals to Rule on Key “Standing” Issue in Data Breach Cases

August 14, 2016

Written by: Sam Crochet, Esq.
Two class actions currently pending in the Third Circuit Court of Appeals, In re Horizon Healthcare Services Inc. Data Breach Litigation and Storm v. Paytime, will impact appellate courts’ future evaluations of “standing.” In Horizon Healthcare, the theft of laptops compromised the information of 839,000 individuals. The Plaintiffs alleged the imminent risk of harm from

[Read Full Article](#)

Judge **Dismisses** **Data Breach** **Class Action** **Against** **Wendy's for** **Lack of** **Standing**

August 11, 2016

Written by Sam Crochet, Esq.
Last month, the defense community scored a victory in the ongoing debate as to when theft of an individual's data becomes a concrete injury for purposes of establishing "standing" to sue. In *Torres v. Wendy's*, the Florida Plaintiff filed a federal class action against the fast food chain following an early-2016 data

[**Read Full Article**](#)

LabMD's Win **Over The FTC** **Is Short Lived**

August 2, 2016

Written by: Richard Sheinis, Esq. On July 29, 2016 the Federal Trade Commission

issued an Opinion and final Order reversing the decision by an Administrative Law Judge (ALJ) that had dismissed FTC charges against medical testing laboratory LabMD, Inc. The Commission concluded that LabMD's data security practices were unreasonable and constituted an unfair trade practice that

[Read Full Article](#)

EU-US Privacy Shield Self-Certification Starts Today

August 2, 2016

Written by: Richard Sheinis, Esq. Today, August 1, is the first day that the U.S. Department of Commerce is accepting self-certifications under the EU-US Privacy Shield. The Privacy Shield, which essentially takes the place of the invalidated Safe Harbor, allows for the transfer of personal information from the EU to the U.S. The self-certification process is

[Read Full Article](#)

The “Internet of Things”: An Inconvenient Truth

August 2, 2016

Written by: Sam Crochet, Esq.
Technology is developing at an explosive pace, which is creating endless opportunities for improvement industry-to-industry. For years we have remotely accessed information from our smartphones, but now we are on the front wave of remotely accessing physical devices themselves. Doctors have the capability of adjusting patients' insulin pumps without the need

[**Read Full Article**](#)

Medjacking, Part 2

July 19, 2016

Written by : Richard Sheinis, Esq. Over the last several months I have written about the dangers of hacker's compromising various types of internet connected medical devices used by hospitals, and other medical providers.

HALL BOOTH SMITH, P.C.

TrapX Security has now issued Part 2 of their “Anatomy of Attack” series, addressing the hacking of medical devices (http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf?alid=1419599). This is

[Read Full Article](#)

HHS Issues Guidance On Ransomware And HIPAA

July 14, 2016

Written by: Richard Sheinis, Esq. On Monday, July 11, HHS issued a “Fact Sheet” on ransomware and HIPAA. While we know that the frequency of ransomware attacks has gone through the roof, HHS brought us some sobering figures. Since early 2016 there have been 4,000 daily ransomware attacks reported in the U.S. This represents a 300%

[Read Full Article](#)

Sixth Circuit

Shuts Down **End Run By** **Plaintiff Using** **A HIPAA** **Breach To** **Claim** **Violations Of** **The False** **Claims Act**

April 19, 2016

Written by: Richard Sheinis,
Esq. The Sixth Circuit Court of
Appeals recently upheld a
dismissal of a lawsuit in which
a plaintiff tried to use the
improper accessing of her
protected health information
("PHI") as a basis for a claim
under the False Claims Act.
In Sheldon v. Kettering Health
Network, 2016 U.S. App.
LEXIS 4236 (2016),

[Read Full Article](#)

4th Circuit **Rules Insurer** **Must Defend** **Insured** **Against Class**

Action Data Breach

April 18, 2016

Written by: Tiffany Winks,
Esq. On Monday, April 11,
2016, the 4th Circuit ruled
in Travelers Insurance v.
Portal Healthcare
Solutions that Travelers had a
duty to defend Portal in a
class action related to Portal
posting patients' medical
records on the internet. A
class action lawsuit was filed
against Portal alleging
patients' medical records
were accessible on

[Read Full Article](#)

Fourth Circuit To Decide If Commercial General Liability Policy Covers Internet Publication of Medical Records

April 1, 2016

HALL BOOTH SMITH, P.C.

Written by: Tiffany Winks,
Esq. On March 24, 2015, the
Fourth Circuit Court of
Appeals heard oral arguments
as to whether a Commercial
General Liability insurance
policy provides coverage for a
data breach. The case on
appeal is Travelers Indemnity
v. Portal Healthcare Solutions,
LLC, 35 F. Supp. 3d 765, (E.D.
Va. 2014). The District Court
had

[Read Full Article](#)

Tennessee **Amends** **Breach** **Notification** **Statute**

March 30, 2016

Written by: Richard Sheinis,
Esq. Senate Bill 2005,
amending Tennessee's data
breach notification law, was
signed by the Governor on
March 24, 2016. The new law
is effective July 1, 2016. The
main changes to the current
law (Tennessee Code
Annotated, Section
47-18-2107) are as follows:
Notification of a data breach
must be provided to affected

[Read Full Article](#)

It Pays to be Ready: HIPAA Phase II Audits Underway Now

March 23, 2016

Written by: Patrick Powell, Esq. On March 21, 2016, the HHS Office for Civil Rights (“OCR”) officially launched Phase 2 of the HIPAA Audit Program. Covered Entities and Business Associates need to be prepared for these audits and be on the lookout for emails from OCR beginning the audit process. The Health Information Technology for Economic

[Read Full Article](#)

If This Does Not Convince You Of The Importance Of HIPAA Compliance, Nothing Will

March 21, 2016

By: Richard Sheinis, Esq. Two

medical providers recently paid large settlements to the Department of Health and Human Services' Office for Civil Rights because of HIPAA violations. Both involved thefts of laptops, an issue I see with some regularity. In one case, The Feinstein Institute for Medical Research in Manhasset, L.I., a research arm for Northwell

[Read Full Article](#)

New Bill To Strengthen Georgia's Data Breach Notification Law Introduced In State Senate

January 27, 2016

Written by: Richard Sheinis, Esq. On January 20, 2016, the "Georgia Personal Data Security Act" was introduced in the State Senate. The current Georgia breach notification law is one of the weakest in the country. It only applies to "information brokers" and "data collectors" that maintain

computerized personal information of individuals. An “information broker”, such as

[Read Full Article](#)

[FDA Issues Draft Guidance for Postmarket Management of Cybersecurity in Medical Devices](#)

January 25, 2016

Written by: Richard Sheinis, Esq. The FDA has issued this draft guidance to add to its other guidance documents on cybersecurity and medical devices, “Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”, and “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”. It is starting to feel like a Harry Potter series. The essence of

[Read Full Article](#)

HHS Clarifies Patients' Right To Health Data

January 15, 2016

Written by: Patrick Powell,
Esq. Under HIPAA, patients
have the right to access and
obtain a copy of their health
information from physicians,
hospitals, and insurers.
However, recent reports have
concluded individuals often
face barriers to accessing
their information, even from
entities required under HIPAA
to provide the data.
Understanding HIPAA's
requirements regarding
patients' access to

[**Read Full Article**](#)

Employee Theft Gives A Lesson In Data Security

January 6, 2016

Written by: Richard Sheinis,
Esq. The Georgia Court of
Appeals just issued an
opinion in a case that
provides a good lesson on the

importance of protecting data against employee theft. In *Lyman v. Cellchem Int'l, LLC*,¹ two former employees of Cellchem were accused of using a thumb drive to copy confidential computer files, including financial data

[Read Full Article](#)

[Preview of the New EU General Data Protection Regulation](#)

December 21, 2015

Written by: Richard Sheinis, Esq. Last week I posted a short blog to let everyone know that a consolidated text of the new EU General Data Protection Regulation (“GDPR”) was released by the European Parliament, and the Council of the European Union. Now it is time to give you a more in depth look at the

[Read Full Article](#)

[EU Provides A Look Into The](#)

New General Data Protection Regulation

December 17, 2015

Written by: Richard Sheinis, Esq. The European Parliament and Council have issued a consolidated text of the new General Data Protection Regulation ("GDPR"). I will be reviewing the text and will provide a complete analysis in the coming days, but this article from the IAPP is a good initial look, <https://iapp.org/news/a/gdpr-we-have-agreement/>. Stay tuned for more analysis, and how

[Read Full Article](#)

Warning of Another Medical Device Vulnerable to Hacking

December 14, 2015

Written by: Richard Sheinis, Esq. In a precursor of things

HALL BOOTH SMITH, P.C.

to come, earlier this month the CERT Division of the Software Engineering institute based at Carnegie Melon University has warned that the Epiphany Cardio Server is vulnerable to hacking. The Cardio Server gathers medical data and diagnostic test results from different medical devices, and makes the

[Read Full Article](#)

[LabMD Defeats FTC](#)

November 17, 2015

Written by: Richard Sheinis, Esq. In a surprising ruling, the FTC has taken a big hit to its self-appointed power to regulate the data security practices of every business in the country. On Friday, November 13, the FTC Chief Administrative Law Judge Michael Chappell dismissed the FTC's complaint alleging that LabMD failed to provide reasonable and

[Read Full Article](#)

[Defending The Technology](#)

Based Medical Malpractice Case Of The Future

November 5, 2015

By: Richard Sheinis, Esq. The medical industry is taking advantage of wireless technology to change the very premise of how case has been provided for hundreds of years. Regardless of whether a doctor was performing bloodletting in the 1700's or an appendectomy in 2000, the one constant was that the patient and doctor always had to

[Read Full Article](#)

EU Court of Justice Declares the US Safe Harbor for the Transfer of Data to Be Invalid

October 6, 2015

Written by: Richard Sheinis,

Esq. In a ruling that can have great ramifications for technology companies, and almost any U.S. company that does business in the EU, the EU Court of Justice has ruled that the Safe Harbor provisions, which for years has allowed companies to transfer personal data from the EU to the U.S., is

[Read Full Article](#)

Obama and Chinese President Reach Agreement to Stop State Sponsored Hacking. Really?

September 29, 2015

Written by: Richard Sheinis, Esq. On Friday of last week, President Obama announced that he and Chinese President Xi Jinping reached a “common understanding” not to conduct or support state sponsored hacking. “We have agreed that neither the U.S. or Chinese government will conduct or knowingly support

cyber-enabled theft of
intellectual property including
trade secrets or

[Read Full Article](#)

Hackers Use Syrian Refugee Crisis to Scam You

September 10, 2015

In a classic case of “social engineering” hackers are using the Syrian refugee crisis to scam people out of money and information. Whenever a humanitarian crises hits, hackers will set up fake websites, send phishing e-mails, and use social media such as Facebook to encourage people to donate money or see the latest news on

[Read Full Article](#)

E-Mail Scam Tricking Businesses Into Wiring Funds to

Hackers Grows 270%

September 5, 2015

This week the FBI said an e-mail scam that tricks businesses into wiring funds to hackers has increased 270% since the beginning of 2015. The FBI has named the scam “Business E-Mail Compromise” or “BEC”. The scam occurs when a hacker infiltrates the e-mail of a company executive. The hacker will then send an e-mail,

[Read Full Article](#)

Third Circuit Rules in Favor of FTC Having Authority to Regulate Data Security

August 26, 2015

On August 24, in FTC v. Wyndham Worldwide Corp., the Third Circuit Court of Appeals found that the FTC had authority to regulate cyber security under the “unfairness” prong of Section

HALL BOOTH SMITH, P.C.

5 of the Federal Trade Practices Act. The background of the case is this: On three (3) occasions in 2008 and 2009 hackers successfully penetrated

[Read Full Article](#)

Cyber Scam Gets Executive to Wire Funds to the Hackers

August 19, 2015

Ubiquiti Networks, Inc. was recently the victim of a cyber scam in which the thieves sent spoof communications to executives to trick them into wiring funds to the fraudsters to the tune of \$46.7 million. Go to Krebs on Security, <http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/>, for a good historical perspective on this scam, but the way it works is this:

[Read Full Article](#)

FDA Urges Hospitals to

Discontinue Use of Hospira Infusion System Due to Cybersecurity Vulnerabilities

August 3, 2015

In a warning that is the first of its kind, on July 31, 2015, the FDA encouraged healthcare facilities to stop using the Hospira Symbiq Infusion System due to cybersecurity vulnerabilities.

(<http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm>) The infusion system is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population. It operates

[Read Full Article](#)

Have the Flood Gates Been Opened for Cyber Breach

Lawsuits?

July 28, 2015

Up until now, most lawsuits against retailers by customers whose personal information was stolen by hackers in a data breach, were dismissed by the courts in the early stages of litigation because the theft of personal information, such as credit card numbers, in and of itself was not considered a sufficient injury to confer “standing”

[Read Full Article](#)

Cyber Cheating on Your Spouse Just Doesn't Pay

July 24, 2015

When I was a kid, my mother would always tell me it doesn't pay to sneak around because I would always get caught. Never has this advice rang so true as when I read about a website for married people seeking affairs that was hacked this week. (Karma?) Avid Life Media, which owns Toronto based

[Read Full Article](#)

Medjacking. . . **Hackers Hi-** **Jacking** **Medical** **Devices**

June 17, 2015

In recent posts I have discussed the need for security to keep hackers from injecting malware into medical devices. Now, TrapX Laboratories has issued a paper on an attack vector called MEDJACK, or “Medical Device Hi-Jack” (<http://trapx.com/solutions/industry-2/healthcare/>). TrapX explains that medical devices are “key pivot points” on a healthcare network. They are the weakest link

[Read Full Article](#)

Building Code **for Medical** **Device** **Software** **Security**

May 29, 2015

HALL BOOTH SMITH, P.C.

Earlier this month I published a Post on, “The Importance of Cyber Security in Telemedicine”, highlighting the importance of security for medical devices that can be hacked. Almost as if on cue, or more likely the result of lucky timing, on May 21, 2015, the IEEE Cybersecurity Initiative (www.cybersecurity.ieee.org) published, “Building Code for Medical Device Software

[Read Full Article](#)

The Importance Of Cyber Security In Telemedicine

May 4, 2015

Telemedicine is coming to a hospital or medical office near you. What is telemedicine? Simply put, telemedicine is when the medical provider is in one location and the patient is in another. The medical professional uses telecommunication technology, often times via the internet, to provide medical care to the patient. Unfortunately, any time

information travels

[Read Full Article](#)

A Tool To Unlock Ransomware

April 20, 2015

As many of you know, ransomware is a malware that infects Windows systems and encrypts files to make them inaccessible and unusable. At the time of the infection, the hacker demands payment in exchange for the decryption key. Even if the ransom is paid, the decryption key is not always received. In a nice development,

[Read Full Article](#)

The Real Reason The FTC Does Not Like The White House's Consumer Privacy Bill

March 25, 2015

In January, President Obama

announced that he would release a draft Consumer Privacy Bill intended to give consumers more control over how data about them is collected and used. The draft Bill was released on February 27, 2015, and already there is no shortage of critics, including the President's own Federal Trade Commission. (<http://wapo.st/192KVXA>) The

[Read Full Article](#)

President's **Big Data and** **Privacy** **Working** **Group Interim** **Report Is** **Troubling**

February 23, 2015

In January 2014, President Obama appointed John Podesta, Counselor to the President, to lead a review of big data and privacy. On February 5, 2015, the Big Data and Privacy Working Group issued an interim report detailing their progress. Unfortunately, the report demonstrates the government cannot resist the temptation to put its clamps

on progress

[Read Full Article](#)

A Simple Lesson for Employers and Employees Courtesy of the Sony Data Breach

December 31, 2014

Many Sony executives are embarrassed, to say the least, by their e-mails, which have been made public as a result of their data breach. (<http://variety.com/2014/biz/news/leaked-sony-emails-reveal-jokes-about-obama-and-race-1201376676/>). I have preached to businesses for a long time that they should make it clear to employees that they do not have an expectation of privacy if they use a

[Read Full Article](#)

The Inevitable Showdown to

Control the Data from Your Fitness App

December 2, 2014

By now, most of us have heard about the health tracking capabilities of HealthKit, part of Apple's latest iPhone operating system, iOS 8. HealthKit offers the ability of users to track and share personal health and medical data such as diet, exercise and activity. The Apple Watch will have a heart rate sensor, GPS, and

[Read Full Article](#)

The Other Wyndham Hotel Case

November 11, 2014

Most of us are aware of the litigation between the FTC and Wyndham Hotels arising out of the data breaches experienced by Wyndham between 2008 and 2010, resulting in hackers stealing the personal information of over 600,000 customers. In a less publicized case arising

out of these data breaches,
Wyndham was sued by a
shareholder

[Read Full Article](#)

FDA ISSUES GUIDANCE ON CYBER SECURITY FOR MEDICAL DEVICES

October 14, 2014

On October 2, 2014, the FDA issued Guidance identifying cyber security issues that manufacturers of medical devices should consider in the design and development of their medical devices, as well as in preparing pre-market submissions for the devices. The goal is to reduce the risk to patients by decreasing the likelihood that device functionality is

[Read Full Article](#)

CALIFORNIA ADDS TO IDENTITY

THEFT **PROTECTION** **LAW**

October 14, 2014

Assembly Bill 1710 has strengthened California's original security breach notification law, first passed in 2003. The Bill expands the applicability of the law to any company that merely maintains personal information of a California resident. The existing law had only been applicable to companies that own or license personal information. Companies that maintain such personal

[Read Full Article](#)

CALIFORNIA **PASSES LAW** **FOR STUDENT** **DATA** **PROTECTION**

October 14, 2014

California Governor Jerry Brown has signed into law Senate Bill 1177, the Student Online Personal Information Protection Act (SOPIPA),

HALL BOOTH SMITH, P.C.

restricting collection and marketing uses of K-12 student data. The Bill requires the operator of an internet website, online service or mobile application to implement and maintain reasonable security procedures and practices to protect the student

[Read Full Article](#)

Yelp and TinyCo Settle FTC Charges of COPPA Violations

October 1, 2014

On September 17, 2014, the FTC announced the review site Yelp, Inc., and mobile app developer TinyCo, Inc., in separate enforcement actions agreed to settle charges that they each violated COPPA.

Yelp agreed to pay a \$450,000.00 penalty, and TinyCo agreed to pay \$300,000.00. COPPA (Children's Online Privacy Protection Act) requires companies that use the

[Read Full Article](#)

Doing Business in Singapore?

July 8, 2014

In the event you collect any personal data while doing business in Singapore, the Personal Data Protection Act in Singapore requires that as of July 2, 2014, organizations collecting and handling personal data in Singapore must have a Data Protection Officer. The Data Protection Officer is responsible for responding to inquiries and complaints relating to

[**Read Full Article**](#)

Verizon 2014 Data Breach Investigations Report Is Here

May 1, 2014

Verizon has released its latest Data Breach Investigations Report, and its 2014 edition is better than ever! Verizon studied 1,367 confirmed data breaches, and 63,437 security incidents in 95 countries. A breach is defined as an incident that results in

the disclosure or potential exposure of data. An incident is a security event that compromises

[Read Full Article](#)

Ponemon Institute Issues its Fourth Annual Study On Patient Privacy & Data Security

March 24, 2014

On March 13 the Ponemon Institute issued its Fourth Annual Study on patient privacy & data security. This study has come to be a respected and well received assessment of the privacy and security of patient information in health care. The study is based upon a survey of 91 health care providers of different sizes.

[Read Full Article](#)

IS HIPAA

READY FOR MEDICAL WEARABLE DEVICES?

March 4, 2014

In technology years, the HIPAA Security Rule is a dinosaur. HIPAA was a brainchild of the enacted in 1996, largely to address health care access, “portability”, and privacy. The final rule on security standards was issued in 2003, to specifically address the security of Electronic Protected Health Information (“PHI”). Where was the Internet and mobility

[Read Full Article](#)

NIST Issues Standards for Critical Infrastructure Cyber Security

February 17, 2014

On February 12, 2013, President Obama issued Executive Order 13636, “Improving Critical Infrastructure Cyber

Security”, which called for a set of industry standards and best practices to help organizations manage cyber security risk. Pursuant to this Order, on February 12, 2014, the National Institute of Standards and Technology (“NIST”) issued the “Framework for Improving Critical

[Read Full Article](#)

What Are You Doing With Your Old Data?

November 11, 2013

As businesses accumulate more and more data, the chances are that a lot of this data becomes old, inaccurate, inactive, stale, or just plain not needed. The recent data breach at Adobe™ is a good lesson in why we should have specific procedures in place to delete data we no longer need. Adobe has offered

[Read Full Article](#)

North Carolina is the Latest

State to Propose Barring Employers from Accessing Employee Social Media Accounts . . . and Why These Laws Can be Troublesome for Business

June 10, 2013

The North Carolina House recently passed the Job and Education Privacy Act (House Bill 846), which would prohibit employers from requesting that an employee or job applicant grant access to their personal electronic account or social networking account. The law would also prohibit employers from tracking an employee's personal electronic communication device, such as

[Read Full Article](#)

HIGHLIGHTS **OF THE 2013** **VERIZON** **DATA** **BREACH** **INVESTIGATI** **ON REPORT**

May 10, 2013

The 2013 Verizon Data Breach Investigation Report is now available. As in past years, the Report provides useful information regarding trends in data breaches, and tips for protecting your company. The following are highlights from the Report: 1. SOURCE OF INFORMATION FOR THE REPORT Verizon receives information from 19 global organizations, including law enforcement agencies,

[Read Full Article](#)

COURTS **REACH** **DIFFERENT** **CONCLUSION** **S IN DATA**

PRIVACY AND **DATA** **BREACH** **CASES** **SEEKING** **CLASS** **CERTIFICATIO** **N**

April 10, 2013

In a tale of two courts, two federal courts have recently gone in opposite directions on the issue of class certification in data privacy and data breach lawsuits. In *In Re Hannaford Bros. Co. Customer Data Security Breach Litigation*, the court refused to certify a class to pursue claims arising out of a data breach of

[Read Full Article](#)

THE **PRESIDENT’S** **EXECUTIVE** **ORDER,** **“IMPROVING** **CRITICAL**

INFRASTRUCTURE SECURITY"... WHAT DOES IT MEAN FOR YOU?

February 20, 2013

On February 12, 2013, President Obama, dissatisfied with Congress' failure to pass legislation to protect the infrastructure that is critical to the Country's operation, signed an Executive Order (EO) titled, "Improving Critical Infrastructure Cyber Security." The immediate questions that pop into the brain trust of many companies are, "Does this apply to us?" and "Do

[Read Full Article](#)

YES IT CAN HAPPEN TO YOU...EMPLOYEE DATA THEFT

February 13, 2013

A recent study by the Ponemon Institute revealed

that employees are causing company's to lose intellectual property (IP) with startling frequency. Perhaps the most troubling aspect of this behavior is the lack of knowledge of the companies that their IP is at risk. The study results, based on survey responses of 3,317 people in the

[Read Full Article](#)

[2012 Verizon Data Breach Investigative Report](#)

April 4, 2012

Each year since 2004, Verizon has released a Data Breach Investigative Report. The 2012 Report (based on 2011 data) is now available. The Report, which contains a compilation and analysis of reported breaches, should be of interest to business owners, insurers, auditors, security experts, and others involved in this field. This Special Edition of Data Protection

[Read Full Article](#)

[Load More Posts](#)

[Subscribe to Our Blog](#)

In the Press

Industry Today: Jade Davis on Artificial Intelligence (AI) for Manufacturing Companies

September 18, 2023

In an article published on September 14, 2023, for Industry Today, Tampa Of Counsel Jade Davis discusses how artificial intelligence (AI) and machine learning can positively impact the manufacturing industry through streamlining and increased efficiency. She also provides insight on how companies can utilize these emerging technologies while mitigating risk. “The cost-benefit of AI makes

[Read Full Article](#)

ED Management: Jade Davis Discusses Emergency Department Unauthorized Records Access

September 14, 2023

In an article for the September 2023 edition of ED Management, Tampa Of Counsel Jade Davis discusses the unauthorized access of records by staff in emergency departments (ED). In it, she touches upon the frequency of these issues, noting that "It is, unfortunately, a recurring dilemma," and that the breaches "tend to be more prevalent

[Read Full Article](#)

E-Crypto News: Danielle Dudai on What's Next

for **Cryptospace** **Following SEC** **Actions**

August 28, 2023

In an article published August 22, 2023, in E-Crypto News, West Palm Beach Of Counsel Danielle Dudai shares her insight on what to expect with crypto regulation as a result of the SEC's actions and recent court decisions. "The concern of course is that the government will try and over-regulate, and eliminate decentralized assets, in

[**Read Full Article**](#)

Daily Business **Review:** **Danielle Dudai** **Reflects on** **the Ripple** **Labs Crypto** **Ruling**

August 23, 2023

In an article published August 17, 2023, in Law.com's Daily Business Review, West Palm Beach Of Counsel Danielle Dudai shares an opposing

view to those who have celebrated the SEC v. Ripple Labs decision as a profound moment for the cryptocurrency community. “Every now and then, a court will issue a ruling that lawyers are

[Read Full Article](#)

Law360: **Richard** **Sheinis on** **Online** **Tracking Tech** **& HIPAA** **Compliance** **Risks**

August 14, 2023

In an article published on August 9, 2023, in Law360, Charlotte Partner Richard Sheinis discusses how increased utilization of technology to track activity online could bring HIPAA compliance risks. “An individual does not have to be a patient of a covered entity, for the covered entity's collection of that individual's information to be PHI. The

[Read Full Article](#)

Hotel **Interactive:** **Richard** **Sheinis on** **Artificial** **Intelligence** **(AI) in** **Hospitality**

July 7, 2023

In a June 25, 2023, article written for Hotel Interactive, Charlotte Partner Richard Sheinis reviews the potential roles artificial intelligence (AI) can play within the hospitality industry. In it, he provides an overview of what AI is, how it works, and what opportunities and risks some popular technologies such as ChatGPT may hold for those

[Read Full Article](#)

Law.com: **Richard** **Sheinis on the** **Rise of Data** **Breach Class** **Actions**

June 28, 2023

HALL BOOTH SMITH, P.C.

In an article published on June 21, 2023, in the New York Law Journal, Richard Sheinis, partner at Hall Booth Smith, and Lisa Jaffe, AVP of Cyber/Technology/Media Claims at Hiscox Insurance, discuss the significant increase in class action lawsuits involving data breaches and how defendants can use legal defenses to stop the class action, such

[Read Full Article](#)

Part B News: **Jade Davis on** **New NIST** **Cybersecurity** **Framework &** **Insurance** **Impact**

April 25, 2023

In an article published on April 10, 2023, in Part B News, Tampa Of Counsel Jade Davis shares her insight and expertise on the Health Care and Public Health Sector Cybersecurity Framework Implementation Guide 2.0, from HHS' Administration for Strategic Preparedness (ASPR), its impact on the industry, and how compliance

could impact cybersecurity
insurance. Davis

[Read Full Article](#)

Journal of Healthcare Risk Management: Richard Sheinis on Geofencing as a Safeguard Against Cyberattacks

December 27, 2022

Hospitals and healthcare systems have long been targets for cyber criminals. One such incident occurred in October 2022 when CommonSpirirt Health announced an IT security incident, leading some such as Richard Shenis, partner and head of the Data Privacy & Cyber Security practice group at Hall Booth Smith, to reiterate strategies such as geofencing as

[Read Full Article](#)

InformationWeek: Richard Sheinis on Protection Against Cyberattacks as Part of the Cost of Doing Business

December 22, 2022

Increasing cyberattacks targeting cultural institutions – including a December 7 attack affecting The Metropolitan Opera’s network systems, website, box office, and call center – have led many to question the purpose of such attacks while some such as Richard Sheinis, partner and head of Hall Booth Smith’s Data Privacy & Cyber Security practice group, simply

[Read Full Article](#)

Journal of Healthcare Risk

Management:
Richard
Sheinis on
Proper
Disposal of
Protected
Health
Information
(PHI)

December 5, 2022

The Office of Civil Rights recently announced a settlement with a Massachusetts dermatology clinic regarding the improper disposal of protected health information (PHI) after staff at the clinic placed empty specimen containers with PHI labels in a garbage bin in their parking lot. Richard Sheinis, partner and head of the Data Privacy & Cyber Security

[Read Full Article](#)

Raconteur:
Richard
Sheinis on

Disconnect Between Cyber Attack Policy Coverage vs. Actual Need

April 14, 2022

In a Raconteur article about the need for companies to ensure they have the right insurance policies to contend with rising cyber attacks, Richard Sheinis, partner and head of the Data Privacy & Cyber Security Service Area at Hall Booth Smith, said “When a client suffers an event, whether that be a ransomware attack or

[Read Full Article](#)

Journal of Healthcare Risk Management: Richard Sheinis on the HIPAA Safe Harbor Law

February 22, 2022

In a Journal of Healthcare Risk

HALL BOOTH SMITH, P.C.

Management article about the HIPAA Safe Harbor Law in which HIPAA-covered entities and their business associates receive certain protections when potentially facing fines and other penalties under HIPAA, Richard Sheinis, Partner and Leader of the Data Privacy & Cyber Security Service Area at Hall Booth Smith, said the law

[Read Full Article](#)

ACC Docket: **Richard** **Sheinis on** **Developing a** **Strategic** **Privacy** **Program** **Across** **Different** **Jurisdictions**

February 11, 2022

In an article published in the Association of Corporate Counsel's ACC Docket, Hall Booth Smith Partner Richard Sheinis and ParkMobile Chief Legal and Privacy Officer Tony Stewart share what it takes to develop a strategic

privacy program that deals with data privacy laws from different jurisdictions. Listed chief in their recommendations are data mapping and

[Read Full Article](#)

Healthcare Risk Management: Richard Sheinis on What Providers Should do When Medical Devices Are Compromised

January 4, 2022

In the January issue of Healthcare Risk Management, Richard Sheinis, Partner and leader of Hall Booth Smith's Data Privacy & Cyber Security Service Area, discusses what health care providers and hospitals should do when a medical device has been compromised. In the article, Richard lays out the steps providers should take when

responding to an

[Read Full Article](#)

Part B News: **Richard** **Sheinis on** **Rising Costs of** **Cyber** **Insurance for** **Health Care** **Providers**

November 24, 2021

In a Part B News story looking at the rising cost of cyber insurance for health care providers and companies as ransomware attacks grow, Richard Sheinis, Partner and Leader of Hall Booth Smith's Data Privacy & Cyber Security Service Area, explains how the market has shifted over time with big payoffs. "Years ago, when a

[Read Full Article](#)

Part B News: **Richard** **Sheinis on**

Potential Health Care Provider OFAC Sanctions

November 2, 2021

In an article published by Part B News on November 1, 2021, Hall Booth Smith Charlotte-based Partner Richard Sheinis discusses the potential sanctions health care providers can incur by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) if they pay a sanctioned international criminal actor as part of a ransomware attack.

[Read Full Article](#)

Law360: Sheinis, Lawrence, & Langhorne on Best Practices to Defend Against Ransomware

August 25, 2021

In an article published online

HALL BOOTH SMITH, P.C.

in Law360 on August 16, 2021, Partner Richard Sheinis and Associates Brett Lawrence and Charles Langhorne offer 17 best practices for companies to defend against ransomware, in light of recent attacks. U.S. businesses were hit with “the biggest ransomware attack on record” in July. “This latest spate of ransomware attacks,

[Read Full Article](#)

Part B News: **Lisa Munoz** **Discusses ONC** **Regulations** **on the** **Protection of** **Patient Data**

March 15, 2021

In an article published by Part B News, Partner Lisa Munoz is quoted discussing the implications of new Office of the National Coordinator for Health IT (ONC) regulations regarding the protection of patient data. While some HIPAA flexibilities have been enacted in response to COVID-19, HIPAA security and privacy rules still require that patients’ protected

[Read Full Article](#)

Healthcare Risk Management: Richard Sheinis on Overturning of \$4.3 Million HIPAA Violation Penalty

February 5, 2021

In an article published by Healthcare Risk Management on February 5, 2021, Partner Richard Sheinis is quoted discussing lessons learned from a \$4.3 million HIPAA violation penalty that was overturned. The penalty was imposed on the University of Texas M.D. Anderson Cancer Center by the Department of Health and Human Services' Office for Civil Rights

[Read Full Article](#)

[Load More Posts](#)